Online Identity Theft on Consumer Purchase Intention: A Mediating Role of Online Security and Privacy Concern

Abdul Bashiru Jibril, Michael Adu Kwarteng, Fortune Nwaiwu, Christina Appiah-Nimo, Michal Pilik, Miloslava Chovancova

Online identity theft on consumer purchase intention: A mediating role of online security and privacy concern

Abdul Bashiru Jibril [0000-0003-4554-0150] Michael Adu Kwarteng [0000-0002-6787-0401]
Fortune Nwaiwu, [0000-0001-8900-2130] Christina Appiah -Nimo [0000-0001-5597-3553]

Michal Pilik [0000-0002-7032-3812], Miloslava Chovancova[0000-0002-9244-9563]

1 Faculty of Management and Economics, Tomas Bata University in Zlin,
Mostni 5139,76001 Zlin, Czech Republic
{Jibril, Kwarteng, Nwaiwu, Appiah-Nimo, Pilik, Chovancova}@utb.cz

Abstract.
This study measures the influence of fear of financial loss (FOFL), fear of reputational damage (FORD), with the mediating effect of online security and privacy concern(OSPCON) towards online purchase intentions in an emerging economy's context. Data was conveniently collected from University students of four of the public higher institutions in Ghana. Out of the 201 questionnaires distributed, 179 were eligible for analysis. A Quantitative methodological approach was adopted which relied on the Partial Least Square approach to Structural Equation Modelling (PLS-SEM) for the statistical analysis. Seemingly, FOFL and FORD constructs were not seen to be a significant direct predictor of online purchase intention. However, the mediating effect of OSPCON for both FOFL and FORD towards online purchase intention in the Ghanaian context was found to be significant, hence the mediated-hypotheses were supported. Nonetheless, we have highlighted the need for additional and further research taking a cue from the study's limitations. The study contributes to our knowledge of how online identity theft practices lead to the unwillingness of online customers to embark on online transactions in an emerging economy, given the rampant outburst of online transactions in the developed world. The originality of this study is in the fact that it focuses on an emerging economy, which is under-researched.

Keywords: Online identity theft, purchase intentions, Security and privacy concern, emerging economy, Ghana

1 Introduction

The saturation of society by new technologies results in increasing levels of adoption and use in daily life activities, this brings with it unprecedented opportunities as well as threats and risks. Information and communication technologies and other related digital technologies especially digital platforms have brought along with them a new dimension to how society is evolving, especially in relation to how people interact and transact business. They have in their own unique way also introduced new challenges

and concerns for users. Some of the challenges and concerns pertaining to the protection of the privacy and sensitive information of users of these technologies. Identity theft is a major example of such challenges faced by users of these technologies, as Cavoukian (2013) noted, identity theft is the fastest-growing form of consumer fraud in North America. The problem of identity theft is not peculiar to North America alone, several authors have reported a growing incidence of this problem around the world (Kahn & Liñares-Zegarra, 2016; Reyns, 2013; Williams, 2016). The issue of identity theft has become ubiquitous especially as a result of the migration of a lot of activities associated with human social and economic activities to online platforms.

This migration of a significant amount of human social and economic activities to online platforms has led to the evolution of the nature and characteristics of identity theft to be in line with the sociotechnical changes currently being experienced by society. Consequently, the regimes of digital safety and security as informed by the threat of online identity theft that has become prevalent globally should not be merely viewed as a political reaction to the risks brought about by the proliferation of digital in society. Rather, online identity theft further constitutes an active threat and factor that influences consumers' purchase intentions especially in developing economies where proactive measures of protection are not particularly up to the standards obtainable in more advanced economies. Thus, where the incipient digital society is collectively re-imagined, negotiated, and created.

Therefore, online identity theft is an issue of major concern for online retailers of goods and services in these developing economy markets where the state of an emerging digital society and the sociotechnical relationships of checks and balances required to govern its emergence are in a constant state of transition (Haddad & Binder, 2019). Though the work by Jordan et al, (2018) replicated some constructs used in this present study to measure the impact of fear of identity theft, perceived risk in online purchase intentions; their work was not narrowed to measure the mediating role of online security and privacy concern that becomes the focal lens of this study. Moreover, their research was neither specific to young students in public higher institutions or to the more definite of an emerging economy's context considered in this paper. We further argue that given the varied and complex reasons manifesting in low levels of eCommerce transactions in the developing world, such as low level of internet penetrations, high levels of income poverty, a high rate of illiteracy, and infrastructural challenges that manifest in logistical inefficiencies even have a repelling effect on purchase intentions. Based on these insights, the current study aims at addressing the prognosis of online identity theft on consumer purchase intentions from a developing economy's perspective by (1) Evaluating the predictive influence of identity theft (FOFL and FORD) towards online transactions (2) Establishing the mediating role of online security and privacy concern (OSPCON) towards online purchase intentions/transactions. Specifically, two research questions emerged:

RQI: What impact does online identity theft have on online transactions from university students in a developing country (Ghana)?

RQ2: What influence does the mediating effect of OSPCON have on online transactions from university students in a developing economy (Ghana)?

The rest of the study is structured as follows: Related works on online identity theft are briefly highlighted. Next, the theoretical foundations of the present study are discussed. Then, the conceptual framework of the study as well as the hypotheses are stated. Methodology and the results are presented. Finally, the study's implication to theory and practice are discussed.

2. Related Works On Online Identity Theft

According to Jordan, Leskovar, and Marič, (2018), a major consequence of the emergence of the internet has been the rise in cybercrime which has accompanied its increasing use as a medium for transacting commercial activities through electronic means. Cybercrime manifests itself invariants that span across a broad range of criminal activities that leverage the electronic exchange of information of users. One of the most pervasive being the incidence of online identity theft which has led to victims suffering significant losses and harm which often leaves them traumatized both emotionally and financially. By applying widely available Internet tools, malicious actors trick unsuspecting computer users into divulging personal data, which is then exploited for illicit purposes, thereby causing mistrust of online payment and banking services Venkatesh, & Goyal, 2010) These malicious individuals often apply techniques such as "phishing" and "pharming" as means of tricking their target victims, this is largely facilitated by the fact that because of the nature of the internet and other electronically mediated interactions, face-to-face contact between interacting parties does not exist or is reduced to the barest minimum. The potential for fraud continues to remain a major obstacle in the evolution and proliferation of e-commerce and online-based financial transactions (Furnell, 2010; Wang & Huang, 2011).

While it is acknowledged that there is no standard definition of identity theft whether it is online or offline (Smith, 2007; Wang & Huang, 2011), for the purpose of this study, it is imperative to examine some definitions identified in literature for the purpose of establishing conceptual clarity that would serve as a guide that would facilitate the achievement of the research objectives. According to Reyns (2013), identity theft is the terminology used in describing the fraudulent use of an individual's personal information for criminal purposes and without the owner's consent. More specifically, Jordan et al. (2018) define online identity theft as an act of online fraud and crimes that involve the duplication of digital information or the high-jacking of online accounts for the purposes of committing identity fraud against individuals or businesses. Also, Cornelius (2016) defines online identity theft as the illicit use of another person's identifying facts for the perpetration of economic fraud or for masquerading another person's identity on the internet.

Online identity theft is prevalent in developed societies as a result of the high levels of internet and mobile penetration in their societies. However, as the levels of internet and mobile penetration continues to rise in developing economies, there is also a corresponding increase in the incidence of online identity theft. Vijaya (2011, p. 237) discusses online identity theft from a developing economy perspective by accessing the impact of phishing attacks which has gained prominence as one of the common techniques frequently employed by criminal elements. He comments that phishing attacks have risen in countries like India, which as of 2009 accounted for 15 percent of all

malicious activity in the Asia-Pacific/Japan (APJ) region, increasing from 10 percent in 2008. He also comments that "for specific categories of measurement in the APJ region, India increased rank in malicious code, spam zombies and phishing hosts from 2008. This made India being the third highest country of spam origin globally."
Ebem, Onyeagba, and Ugwuonah (2017, p. 2) reveal that "despite the giant strides and achievements of internet banking, the Nigerian financial sector is currently battling with the twin evils of identity theft and financial frauds, just like other advanced economies of the world". Also, Ladan (2014, p. 17) conducted research which reviewed recent developments in cyberlaw responses to cybercrime and cybersecurity in Nigeria and the economic community of West African States (ECOWAS), from the findings of his research, he established that "online identity theft which includes the act of capturing another person's credentials and/or personal information via the Internet with the intent to fraudulently reuse it for criminal purposes is now one of the main threats to further deployment of e-government and e-business services in Nigeria and across the West African sub-region". Hence, these observations make it imperative to understand the phenomenon of online identity theft from the perspective of developing economies, especially in relation to its impact on consumer purchase intentions.
However, for the sake of argument, and also towards the nature and rationale of this study, we will be limiting the investigation to the mechanism of online security and privacy concern as a risky component of influence in online identity theft in a developing context. In framing our arguments, we have been inspired by the scale of the validated construct of Fear of reputational damage and Fear of financial loss by Hille, Walsh, & Cleveland (2015).

2.1 Conceptual Model Development and Research Hypotheses

2.1.1 The relationship between fear of financial loss, Online security and privacy concern, and Online customer purchase intention

According to Gurung and Raja (2016), concerns about privacy protection is one of the primary obstacles for consumers to participate in electronic eCommerce transactions that require them to divulge personal information, such as their date of birth, social security number, personal phone number, and credit card information, etc. 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 (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 online shoppers 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. Hence, based on evidence in order to extend the scope of understanding based on scientific evidence, the following hypothesis is proposed as a basis to investigate the causal relationship between fear of financial loss and online customers' purchase intentions, this will be done by looking at the mediating effects (if any) of online security vis-à-vis privacy concerns

H1: Fear of financial loss will predict online customers' purchase intentions via the mediating effect of online security and privacy concern.

H3: Fear of financial loss directly affects online customers' purchase intention.

2.1.2 The relationship between fear of reputational damage, online security and privacy concern, and online purchase intention

As consumer patronage via online shopping medium continues to increase, there are still doubts and restraining factors that impact on the consumers' behavioral intentions and willingness to use such systems. 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. As part of scientific inquiry that aims to investigate the relationships between fear of reputational damage and issues such perceived risk associated the intentions to embark on online transactions from the consumers' perspective, results from the research conducted by Jordan et.al. (2018) showed that there is a positive correlation in the relationship between fear of financial losses, fear of reputational damage, perceived risk, and the relation between the constructs of perceived risk and online purchase intention was negative. Their research 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) and that of Jordan et al., (2018). Consequently, this research further aims to investigate specifically, how the fear of reputational damage influences online consumers' purchase intentions with online security and privacy concerns as mediating effects. Hence, the relevant hypothesis is proposed as follows

H2: Fear of reputation damage will predict online customers 'purchase intentions via the mediating effect of online security and privacy concern

H4: Fear of reputational damage directly affects online customers' purchase intention.

To conclude, we deduced a conceptual model, as well as the summary of research constructs and their measurement items from the literature, are given below in Figure 1 and Table 1 respectively.

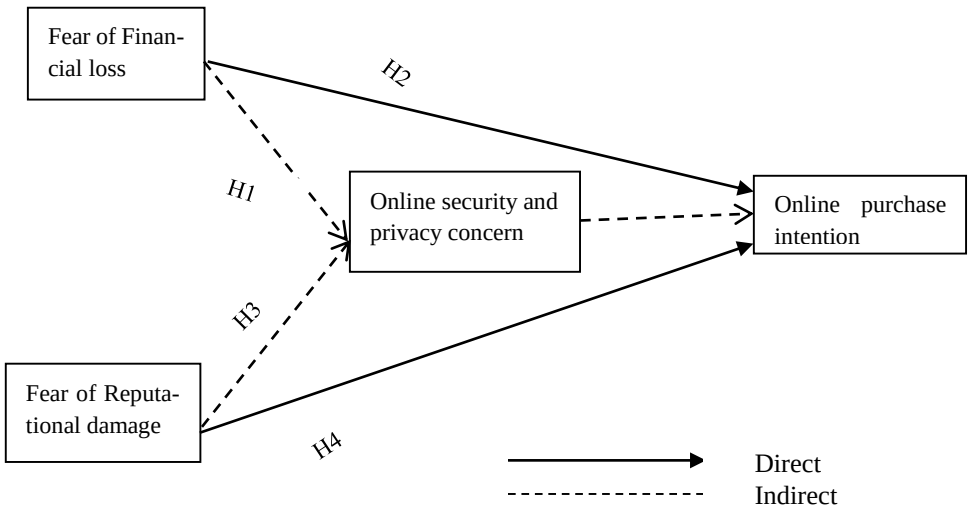

Figure 1: Conceptual model

3 Methodology

Data was conveniently collected from University students of four of the public higher institutions in Ghana. Out of the 201 questionnaires distributed, 189 were eligible for analysis. Survey respondents were pre-qualified to ensure that their knowledge of online buying or shopping, as well as its accompanying online theft and cybercrime instances, was adequate to answer the survey questions. Data collection was undertaken in the months between June to September 2019. On average, the questionnaire took 10 minutes to fill. As earlier stated, the respondent positions comprised: University students in some selected public higher institutions in Ghana (University of Cape Coast(UCC), University of Ghana (UG), Kwame Nkrumah University of Science and Technology (KNUST), and the University for development studies (UDS)) and more particularly undergraduate students who frequently visit the Internet - daily and/or weekly activity. This was made possible as a result of getting a fair representation of university students across the length and breadth in Ghana. We must emphasize that all the selected universities are dispersed in all the three belts in Ghana, thus the Northern, Southern, and Middle belt of Ghana.

Partial least squares (PLS) path modeling was used to simultaneously estimate both the measurement and structural components of the model. The model is shown in Figure 2 (see appendix A) was analyzed using SmartPLS software. Furthermore, our work is consistent with most of the views expressed in Podskaoff et al. (2003) regarding the minimization of common method variance.

3.1 Constructs Measurement

In line with previous studies, this study adapted constructs from existing studies. The measures for FOLF, FORD were based on the works of Hille, Walsh, & Cleveland (2015); Doherty, Ellis-Chadwick, Allred, Smith, & Swinyard (2006), while the measure of OSPCON was mostly culled from the works of Tan, Chong, Loh, & Lin, (2010). Hille, Walsh, & Cleveland (2015) and Ajzen (1991). Finally, the measure of OPI was sourced from; Fishbein and Ajzen 1975; Duan, Edwards, & Dwivedi, 2019; Venkatesh et al, 2003, and Hille, Walsh, & Cleveland (2015). Readers should also note that measurement items were anchored on a six-point scale with 1 - being completely agreed and 6 - completely disagree.

4 Results

4.1 Model fit tests

Assessing measurement models is the initial step in performing any PLS-SEM. This stage confirms that indicator variables (unobserved) are actually measuring constructs (observed variables) they ought to do. Therefore, we assessed our measurement model using convergent validity, and reliability following the suggestion of Hair et al. (2014). Consistent with recent investigations, and also acknowledging the initial step in evaluating PLS-SEM results as earlier suggested, the measurement model must be first assessed, using the indicator loadings (see Hair et al, 2017a). With this in mind, loadings

of approximately 0.708 are deemed fit since they best explain more than 50 percent of the indicator variance, hence providing an acceptable threshold for item reliability. Going by this rule of thumb, all items associated with our indicator reliability exhibited more than 50 percent of the indicator cross-loadings which suggest the level of associations (items correlation) to their respective construct (see Table 2).
For internal consistency reliability, both Cronbach alpha (CA) and the composite reliability (CR) were used as a metric in the assessment. With a minimum threshold and a rule of thumb recording 0.5 and 0.6 respectively (see Bagozzi and Yi, 1988). Therefore, both CA and CR exceeded the baseline recording as follows for all the latent constructs as 0.92, 0.93 respectively for FOFL, 0.86, 0.91 respectively for FORD, 0.84, 0.91 respectively for OPI and 0.89, 0.93 respectively for OSPCON. For convergent validity, the Average Variance Extracted (AVE) was used to measure the extent to which the constructs congregate in order to explain the variance of all items on each construct (Hair et al, 2019). However, the minimum acceptable AVE is 0.50 or more, thus an indication of 50 percent or more on how the variance of items makes up with the specified construct. Reflecting on this threshold, all AVE for our latent constructs exceeded the minimum acceptable baseline (see Table 2) for more details.

Table 2: Item loadings

	Construct			
Items	FOFL	FORD	OPI	OSPCON
FOFL1	0.745003			
FOFL2	0.740739			
FOFL3	0.756215			
FOFL4	0.870122			
FOFL5	0.832757			
FOFL6	0.858748			
FOFL7	0.902154			
AVE =0.668216 *CR= 0.933411* *CA=0.917131*				
FORD1		0.869112		
FORD2		0.828146		
FORD3		0.830033		
FORD4		0.834515		
AVE =0.706638 *CR= 0.905937* *CA= 0.862968*				
OPI1			0.769416	

OPI2	0.91521	
OPI3	0.905006	
AVE =0.749549 *CR= 0.899249* *CA= 0.841929*		
OSPCON1		0.918411
OSPCON2		0.919658
OSPCON3		0.858576
AVE =0.808801 *CR= 0.926888* *CA= 0.884311*		

Note: AVE =Average variance extracted, CR= Composite reliability,
CA= Cronbach's Alpha

Sources: Authors' estimation from SmartPLS

4.2 Test of structural model: A mediation analysis

Following the validity of the measurement model, assessment of the structural model is necessary since it justifies the model's ability to predict the endogenous variables or dependent variables. Therefore, the assessment of the structural model follows a procedure which took inspiration from (Hair et al., 2017) in order to advance issues in partial least squares structural equation modeling. To proceed, it is important to remind readers that the focal point of this study was to measure the mediation of OSPCON on FOFL and FORD towards OPI consequently the direct effect of OSPCON on the former. To accomplish this, we examined two direct relations, namely, *H2 and H4* whiles the remaining hypothesized scenarios were centered on the observation of mediated relationship (i.e.*H1 and H3*). Going by our empirical estimates, our findings from the direct relationships revealed that FOFL has a positive coefficient but a weak predictor of OPI. However, the bootstrapping t-test (with t*>1.96 as significant level), but our estimate indicated an insignificant direct relationship (*β=0.099, t=0.649)* between FOFL and OPI which therefore does not offer empirical support for H2 (See Table 2 for more details). With respect to *H4*, our estimate also suggested that FORD though positive and weak predictor of OPI, but also insignificant (*β=0.165, t=0.665*) indicating that H4 was not supported. With the mediated observations, it can be seen from Table 3 that OSPCON as a mediator to both FOFL and FORD towards OPI are all supported (*H1 and H3*), thus, statistically recording as follows: FOFL -> OSPCON -> OPI= (*β=0.418, t* = 4.594) and FORD -> OSPCON-> OPI= (β=0.392, t* =3.740*) as shown from Table 3 below.

Table 3: Direct and Indirect effect on online identity theft.

Direct and Indirect Effect (Hypothesis)	Path coefficient (β)	T-test (Bootstrapping)	Decision

(H2) FOFL -> OPI	0.099	0.649	Not supported
(H4) FORD -> OPI (H4)	0.165	0.665	Not supported
(H1) FOFL -> OSPCON -> OPI	0.418	4.594*	Supported
(H3) FORD -> OSPCON-> OPI	0.392	3.740*	Supported

t* > 1.96 equal p-value < 0.05 significant level
(Readers should note that the significance testing has been executed using the bootstrapping procedure)

Sources: Authors' estimation from SmartPLS

5 Discussions

Research Question one:
This question, addresses whether there is a direct relationship amongst FOFL, FORD, and OPI in an event of online identity theft towards online transactions amongst university students in a developing country (Ghana)? With the general 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 inconsistent with the study of Mitchison et al, (2004) that 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. Disputing the claims by Mitchison and co, the present study does elucidate the tendency that FOFL will predict or affect the customers' decision to engage in online transactions in an emerging economy. Again, with the research works of Jordan et al, (2018) regarding FOFL and FORD relative to the OPI, their study turned out to have positive relationships 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, (2015) stating that FOFL has a stronger magnitude of effect on OPI than FORD whiles our present study refutes this claim by reporting that the two constructs have no positive or direct relations with OPI. Alternatively, in their findings from study 3 of the same research works of Hille et al, (2015), it was established that FORD does not play a significant major role in affecting OPI.

Research Question two:
Research Question two addresses whether there is an influence on the mediating role of OPSCON towards online transactions amongst university students in a developing economy (Ghana) context. Concerning H1a as earlier stated, the authors propose that the positive or direct link between FOFL and OPI will be mediated by OPSCON, our research estimate, however, establishes support for H1a (See Table 2). This finding,

though largely studied under different contexts in literature, mirrors with previous research works in the risk concerning online buying behaviour (see Hong and Cha, 2013; Miyazaki and Fernandez, 2001; Chuang and Fan, 2011). 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 as a conduit of online purchase intentions; reflecting on the notion of online identity theft circumstances.

5.1 Limitations and Future research

While the present study adds to the existing body of knowledge in the perceived risk associated with online transactions by examining the given model between the online customers considering an emerging economy, several limitations are present that remain to be addressed and creates an avenue for future research. First, the sample has 189 respondents. Adding to this limitation is the fact that, the study was conducted using a student population and so makes it difficult to generalize beyond the target population.

Although the sample is well enough, this sample is somewhat below the recommendations of the pioneer scholars well versed with the application of the structural equation model (Hair et al,2017). Future research should consider augmenting the sample size for the given model. The second limitation of the study is geared towards the failure to address the question of potential experience of the respondents. Future works should include a construct to measure the experience from online identity theft from the developing or emerging economy's perspective.

5.2 Concluding Observations

The aim of the study was to develop and test a theoretical framework bent on eliciting the notion of online identity theft on consumer purchase intention via the mediating role of online security and privacy concern; within a sub-Saharan African context (Ghana). Like the emerging concept of online buying behavior in developing context, the study explores the relationships of both direct and indirect effect of FOFL and FORD towards OPI whiles OSPCON are mediated towards the former. While the study finds no support for 2 direct links with 2 support of the mediated variable, this study highlights the differences between online identity theft on one hand and its associated online intentions on the other hand. While this study is able to predict customers' in an emerging economies fear of online identity theft towards their zeal to embark on online transactions, specifically using three major constructs i.e. FOFL, FORD, and OSPCON. In sum, this study provides a strong reference point to continue to broaden the literature in the developing economy so far as online transactions are concerned, arguing that the internet is not leaving in extinction any time soon.

Acknowledgment

This work was supported by the Internal Grant Agency of FaME through TBU in Zlín No. IGA/FaME/2019/008; and further by the financial support of research project NPU I no. MSMT-7778/2018 RVO - Digital Transformation and its Impact on Customer Behaviour and Business Processes in Traditional and Online markets.

References

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In Action control (pp. 11-39). Springer, Berlin, Heidelberg.

Ajzen, I. (1991). The theory of planned behavior. Organizational behavior and human decision processes, 50(2), 179-211.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. Journal of the academy of marketing science, 16(1), 74-94.

Cavoukian, A. (2013). Privacy by Design and the Promise of SmartData BT - SmartData. In I. Harvey, A. Cavoukian, G. Tomko, D. Borrett, H. Kwan, & D. Hatzinakos (Eds.) (pp. 1–9). New York, NY: Springer New York.

Chuang, H.M. and Fan, C.J., 2011. The mediating role of trust in the relationship between e-retailer quality and customer intention of online shopping. African Journal of Business Management, 5(22), pp.9522-9529.

Cornelius, D. R. (2016). Online identity theft victimization: An assessment of victims and non-victims level of cyber security knowledge. ProQuest Dissertations and Theses. Colorado Technical University, Ann Arbor. Retrieved from https://search.proquest.com/docview/1870624251?accountid=15518

Doherty, N. F., Ellis-Chadwick, F., Allred, C. R., Smith, S. M., & Swinyard, W. R. (2006). E-shopping lovers and fearful conservatives: a market segmentation analysis. International Journal of Retail & Distribution Management.

Duan, Y., Edwards, J. S., & Dwivedi, Y. K. (2019). Artificial intelligence for decision making in the era of Big Data–evolution, challenges and research agenda. International Journal of Information Management, 48, 63-71.

Ebem, D. U., Onyeagba, J. C., & Ugwuonah, G. E. (2017). INTERNET BANKING: IDENTITY THEFT AND SOLUTIONS - THE NIGERIAN PERSPECTIVE. Journal of Internet Banking and Commerce, 22(2), 1–15. Retrieved from https://search.proquest.com/docview/1949087351?accountid=15518

F. Hair Jr, J., Sarstedt, M., Hopkins, L., & G. Kuppelwieser, V. (2014). Partial least squares structural equation modeling (PLS-SEM) An emerging tool in business research. European Business Review, 26(2), 106-121.

Fishbein, M. (1981). leek Ajzen (1975), Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research. Read-ing, MA: Addison-Wesley.

Furnell, S. M. (2010). Online identity: Giving it all away? Information Security Technical Report. https://doi.org/10.1016/j.istr.2010.09.002

Gurung, A., & Raja, M. K. (2016). Online privacy and security concerns of consumers. Information & Computer Security, 24(4), 348-371.

Haddad, C., & Binder, C. (2019). Governing through cybersecurity: national policy strategies, globalized (in-) security and sociotechnical visions of the digital society. Österreichische Zeitschrift Für Soziologie, 44(1), 115–134. https://doi.org/10.1007/s11614-019-00350-7

Hair Jr, J. F., Sarstedt, M., Ringle, C. M., & Gudergan, S. P. (2017). Advanced issues in partial least squares structural equation modeling. Sage Publications.

Hair, J.F., Risher, J.J., Sarstedt, M. and Ringle, C.M., 2019. When to use and how to report the results of PLS-SEM. European Business Review, 31(1), pp.2-24.

Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. Journal of Interactive Marketing, 30, 1-19.

Hong, I.B. and Cha, H.S., 2013. The mediating role of consumer trust in an online merchant in predicting purchase intention. International Journal of Information Management, 33(6), pp.927-939.

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/http://dx.doi.org/10.2478/orga-2018-0007

Kahn, C. M., & Liñares-Zegarra, J. M. (2016). Identity Theft and Consumer Payment Choice: Does Security Really Matter? Journal of Financial Services Research. https://doi.org/10.1007/s10693-015-0218-x

Ladan, M. T. (2014). REVIEW OF RECENT DEVELOPMENTS IN CYBERLAW RESPONSES TO CYBERCRIME AND CYBERSECURITY IN NIGERIA AND THE ECONOMIC COMMUNITY OF WEST AFRICAN STATES (ECOWAS). Law Technology, 47(4), 14–84. Retrieved from https://search.proquest.com/docview/1656056536?accountid=15518

Martín, S. S., Camarero, C., & José, R. S. (2011). Does involvement matter in online shopping satisfaction and trust? Psychology & Marketing, 28(2), 145-167.

Mitchison, N. et al. (2004), Identity Theft: A Discussion Paper, European Commission Joint Research Center, March 2004, [online] Available at https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf

Miyazaki, A.D. and Fernandez, A., 2001. Consumer perceptions of privacy and security risks for online shopping. Journal of Consumer affairs, 35(1), pp.27-44.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. Journal of applied psychology, 88(5), 879.

Reyns, B. W. (2013). Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses. Journal of Research in Crime and Delinquency. https://doi.org/10.1177/0022427811425539

Smith, R. (2007). Cybercrime and Society. Australian & New Zealand Journal of Criminology. https://doi.org/10.1375/acri.40.3.360

Tan, K. S., Chong, S. C., Loh, P. L., & Lin, B. (2010). An evaluation of e-banking and m-banking adoption factors and preference in Malaysia: a case study. International Journal of Mobile Communications, 8(5), 507-527.

Venkatesh, V., & Goyal, S. (2010). Expectation disconfirmation and technology adoption: polynomial modeling and response surface analysis. MIS quarterly, 281-303.

Vijaya, Geeta, D. (2011). Online identity theft – an Indian perspective. Journal of Financial Crime, 18(3), 235–246. https://doi.org/10.1108/13590791111147451

Wang, B. S. K., & Huang, W. (2011). The Evolutional View of the Types of Identity Thefts and Online Frauds in the Era of the Internet. Internet Journal of Criminology.

Williams, M. L. (2016). Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level. British Journal of Criminology. https://doi.org/10.1093/bjc/azv011