THE IMPACT OF ONLINE IDENTITY THEFT ON CUSTOMERS' USAGE INTENTION OF E-BANKING TRANSACTIONS IN UNCERTAIN CONTEXT

Thanh Tam Le [*], Do Thu Ha Tran [*], Mai Khanh Nguyen [*], Le Hoang Giang Do [*], Quynh Trang An [*], Hoang Minh Chu [*], Manh Dung Tran [*], Thi Thanh Nhan Nguyen [**]

* National Economics University, Hanoi, Vietnam
** *Corresponding author*, Haiphong University, Hai Phong, Vietnam
Contact details: Haiphong University, 171 Phan Dang Luu, Hai Phong, Vietnam

OPEN ACCESS

How to cite this paper: Le, T. T., Tran, D. T. H., Nguyen, M. K., Do, L. H. G., An, Q. T., Chu, H. M., Tran, M. D., & Nguyen, T. T. N. (2023). The impact of online identity theft on customers' usage intention of e-banking transactions in uncertain context. *Journal of Governance & Regulation, 12*(4), 60–71.
https://doi.org/10.22495/jgrv12i4art6

ISSN Online: 2306-6784
ISSN Print: 2220-9352

Received: 10.02.2023
Accepted: 16.10.2023

JEL Classification: F65, G01, G34, O16
DOI: 10.22495/jgrv12i4art6

Abstract

During the fierce national and international competition, many organizations are taking digital technology into action to provide new products to customers via modern interactive channels (Sepashvili, 2020). This research is conducted to provide empirical evidence on the effects of online identity theft on consumers' usage intention to engage in e-banking transactions in uncertain context. Using structural equation modeling (SEM) and survey data from 441 individuals, the main findings of the study are: 1) Security and privacy concerns (SAPC) should be divided into two sub-factors: a) e-banking security and privacy concerns, and b) internet security and privacy concerns. It differs from previous studies that combined the Internet and e-banking. We found that *trust* (*T*) is negatively impacted by Internet concerns and positively impacted by e-banking concerns; 2) Trust positively impacts the usage intention of e-banking (UIEB); 3) Fear of online identity theft (FOIT) has a positive effect on trust; 4) FOIT positively impacts SAPC. Theoretically, this study has focused on investigating potential determinants influencing customer intention when gradually adapting to new technology services. In practice, the proposed study will go into depth on the limitations faced by clients in the hidden dimension, which prevent them from engaging in online banking activities.

Keywords: E-Banking, Online Identity Theft, Usage Intention, Uncertain Context, Vietnam

Authors' individual contribution: Conceptualization — T.T.L., D.T.H.T., M.K.N., L.H.G.D., Q.T.A., and H.M.C.; Methodology — T.T.L., D.T.H.T., M.K.N., L.H.G.D., Q.T.A., and H.M.C.; Software — M.K.N. and L.H.G.D.; Validation — D.T.H.T., M.K.N., and L.H.G.D.; Formal Analysis — M.K.N. and D.T.H.T.; Writing — Review & Editing — T.T.L., M.D.T., and T.T.N.N.; Visualization — M.K.N. and L.H.G.D.; Supervision — T.T.L.; Funding Acquisition — T.T.L. and M.D.T.

Declaration of conflicting interests: The Authors declare that there is no conflict of interest.

1. INTRODUCTION

Most financial and commercial transactions are already carried out electronically as a result of the development of information technology and digital communication. Electronic devices have become essential to facilitating e-commerce thanks to the advancement of information technology (Alkrisheh, 2022). Therefore, e-banking has gradually become a familiar term in the banking system in Vietnam. Ting et al. (2016) state that the limitations of conventional payment systems have caused the expansion of e-commerce to change how some financial obligations are paid. Technological advancements in financial intermediaries are critical to addressing the diverse range of customer requirements and adjusting to the digital era (Ajide, 2016). Moreover, in the context of uncertainty, the demand of digital technology solutions for banks became increasingly obvious. Vietnam and the world in general have gradually had to adapt to the emergence of COVID-19. The pandemic's consequences have changed consumers' short and long-term payment and buying decisions. As a result, electronic banking is regarded as an important technique for dealing with severe competition in the financial system and commercial banks (Al-Smadi, 2012). All banks tend to view that digital transformation is fundamental, hence most banks have been building development strategies based on 4.0 technologies and developed services on online and mobile banking. In the period of 2022–2025, the online banking market in Vietnam considered to have greater potential for growth because of the increase in the number and quality of e-payment users in Vietnam.

In response to the increasing demands of corporate entities and the challenges of the contemporary world, the financial system has had to adapt and modernize as a result of that expansion, which evolved in more complicated business models and new types of risk (Ajide, 2016). With the advent of e-banking, cybercrime in Vietnam has given rise to a slew of complex difficulties with financial transactions. Although the variables influencing customers' intention to engage in e-banking services in Vietnam have been examined, there are few studies that specifically address online identity theft. Concerns about online identity theft are growing, especially in a variety of risky scenarios. The crimes began to emerge on the network and have increased over time. They already take many different forms, including hacking websites to access information, destroying, or capturing it to then steal the data or information, or simply altering it by using viruses (Alkrisheh, 2022). This fear is divided into three groups, which are named: 1) fear of financial loss, 2) fear of reputational damage, and 3) concerns related to security and privacy respectively (Jibril et al., 2020). Recently, rising numbers of individuals are duped by criminals in order to carry off information and take their possessions. This has partly affected consumers' decision to use e-banking, it results in loss of funds and loss of belief in keeping money at the bank. Vietnamese customers are particularly susceptible to cybercrime in the financial sector since more than 48% of them appear to be aware of cybercrimes and the services banks offer to inform them of their transactions. However, more than 50% lack thorough understanding about or access to any preventative measures for cybercrime (Tam et al., 2020). To sum up, it cannot be denied that customer fears of online identity theft may indeed influence customer propensity to engage in e-banking transactions. For this reason, banks also need effective policies to increase loyalty and attract customers' attention to their services.

The research is aimed at: 1) determining the factors affecting the intention to participate in e-banking transactions in the context of Vietnam's economic unpredictability; 2) analysing the impacts of online identity theft; and 3) suggesting some certain solutions which should be considered for application to banks, customers, and policymakers.

The structure of this paper is as follows: Section 1 introduces the urgency of the research. Section 2 reviews the relevant literature review. Section 3 analyses the research methodology that has been used to conduct empirical research. Section 4 refers to research results and Section 5 discusses the correlation between variables. Finally, Section 6 has a conclusion and suggests some recommendations for commercial banks, clients and policymakers.

2. LITERATURE REVIEW

2.1. Concepts used through the study

Electronic banking (also known as e-banking) represents an apparent transformation in the 4.0 technology era of banks around the world. People also refer to e-banking by its other names, such as "*virtual banking*", "*online banking*", "*cyber-banking*", "*web banking*", "*phone banking*", and "*remote electronic banking*" (Shannak, 2013). Currently, different concepts of e-banking are defined in numerous studies worldwide. In this study, *e-banking* is defined as all forms of transactions between banks and customers based on the processing and transferring of digitized data to deliver banking services through the Internet (Maditinos et al., 2013). By using this form of banking, customers can: 1) transfer funds, 2) pick up the cheque, 3) pay for mobile airtime, 4) send money to most anyone, 5) take complete control of their account including their balance or transaction alerts (Mori & Mlambiti, 2020). Therefore, customers may utilize the websites of their banks to conduct common banking tasks including getting information on account balances, interest and currency rates, money online transactions (bills, normal payments), and printing receipt (Lin et al., 2014). When users use the Internet to access their e-banking accounts and complete financial transactions, they are doing e-banking (Lin et al., 2014).

Usage intention is defined as a desire to participate in a certain action (Ajzen, 1991). Someone will engage in an activity if they wish or intend to do so (Ajzen, 1991; Jogiyanto, 2007). *The intention* is a mental state that indicates a commitment to carry out a future action or activity. Mental actions such as planning and thinking are involved in intention. The intention to use e-banking service is viewed as the motive for performing an action, making a decision on whether to use or not to use the e-banking service in

the future. There are three indicators for usage intention, including: 1) usefulness, 2) trust, and 3) applicability (Venkatesh, 2000).

Uncertain context is the context of complicated developments of the epidemic and macro fluctuations. People's views regarding any occurrence in their environment, including the purchase and kind of items, shift in response to strict closure and anti-COVID-19 efforts (Bytyçi et al., 2021). In addition, inflation has a negative influence on macro fluctuations in gasoline prices, stock market, gold market, and a crisis in the foreign exchange market (money value decreased). Furthermore, trade tensions between major economies are still complicated, even escalating quite quickly at some points. The biggest example is the United States (US)–China trade war. The next development of the trade war is still exceedingly difficult to predict because the reason of the conflict is not only on trade issues. Trade tensions would depress trade, disrupt global supply chains, and divert trade away from developing countries.

Online identity theft is defined as an act of online fraud and crimes that involve the unlawful duplication of digital information or the high-jacking of another person's identifying accounts (name, birth date, address, credit card number) on the Internet to commit economic fraud or for masquerading another person's identity on the Internet (Reyns, 2013; Cornelius, 2016; Jordan et al., 2018). Online identity theft is a cybercrime that frequently involves stealing another person's personal or financial information. Transactions need customers transferring their personal and financial information to third parties (Forsythe et al., 2006). Online transactions necessitate sharing personal and financial information with third parties (Forsythe et al., 2006). The collected information is subsequently exploited for personal advantage, frequently by making purchases or selling someone's identity or credit card information to the highest bidder online (Jibril et al., 2020). Online identity theft is a burgeoning problem that affects people around the world (Reyns & Henson, 2015). Because of the lower cost of data transmission and developing technologies, it is now simpler to obtain and distribute clients' personal information with the third parties (Clay & Strauss, 2000). Berghel (2000) claimed that identity theft may devastate personal credit and potentially lead to highly expensive legal action that can take years, if not decades, to properly remedy or restore what has been lost.

2.2. Components of online identity theft

Fear of online identity theft (FOIT) is "an emerging negative consumer emotion activated through consumers' cognitive appraisal/own thoughts regarding the possibility of the theft of personal and financial data when conducting transactions online" (Hille et al., 2015, p. 2). FOIT occurs when the individual fears that a third party could steal his/her identity in a transaction regarding any related e-business (Lai et al., 2012). Adopting that customers are afraid of financial losses and their reputations being damaged (van der Meulen, 2006), two dimensions of the "*fear of online identity theft*" proposed by Hille et al. (2015) included fear of financial loss (FOFL) and fear of reputational damage (FORD).

Security and privacy concerns (SAPC) is defined as "the Internet customer's concern for controlling the acquisition and subsequent use of the information" (Castañeda & Montoro, 2007, p. 3) as well as the security systems that protect their personal information on the Internet (Belanger et al., 2002). SAPC occur when customers have to divulge their personal information, such as their: 1) date of birth, 2) social security number, 3) personal phone number, 4) credit card information, and 5) account details, among others (Jibril et al., 2020). In this research model, SAPC is hypothesized to be affected by the FOIT and simultaneously affect the intention to use e-banking.

Trust is a deeply ingrained idea, expectation, or feeling arising in the individual's early psychological development (Jibril et al., 2020; Walsh et al., in press). Online trust is defined as the consumer's "trust in the infrastructure and the underlying control mechanism (technology trust) which deals with transaction integrity, authentication, confidentiality, and non-repudiation" (Ratnasingam et al., 2002, p. 384). Besides, trust is defined as the willingness of consumers to participate in e-commerce with the belief that the companies will not misuse their personal information (Gurung & Raja, 2016). This factor is hypothesized to be affected by FOIT and SAPC as well as the usage intention of e-banking (UIEB).

2.3. Relationship between fear of online identity theft, security and privacy concerns, and usage intention

In terms of the relationship between fear of online identity theft (FOIT), security and privacy concerns (SAPC), and usage intention, security and privacy concerns have been found to have a negative relationship with the customer's intention to participate in online shopping in particular (Udo, 2001) and the adoption of e-commerce in general (Vasileiadis, 2014; Gurung & Raja, 2016; Boateng et al., 2016). Moreover, SAPC have been discovered to negatively affect the intention to adopt and use e-banking services (Sathye, 1999; Lafraxo et al., 2018). It is obvious that the major reason customers are hesitant to engage in e-banking transactions is that the internet's security systems are not safe enough to make them feel confident in performing personal business.

Security and privacy concerns has also been placed as a mediator in the relationship between online identity theft and the intention to use e-banking in the research of Jibril et al. (2020). In the study by Jibril et al. (2020), FOIT has a positive effect on SAPC, while SAPC has no substantial impact on the usage intention of e-banking. In the study of Hille et al. (2015) and Jordan (2018), FOIT negatively correlates with online purchase intention.

2.4. Relationship between security and privacy concerns, trust, and usage intention

Trust is a factor directly affected by security and privacy concerns (Vasileiadis, 2014). Research results by Vasileiadis (2014) indicate that SAPC have a positive relationship with trust. When e-banking users' privacy and security concerns decrease since their account is protected by superior security, they tend to put more trust in the bank where they use their financial services.

In the research of Nwaiwu et al. (2020), Trust is considered a critical factor influencing behavioral intention. Previous research has studied the positive impact of trust in a range of contexts, such as: 1) online purchase intention (Gefen et al., 2003; Amoroso & Hunsinger, 2009; Hille et al., 2015); 2) user's willingness to engage in online exchanges of money and sensitive personal information (Hoffman et al., 1999; Wang et al., 2003); 3) e-banking adoption (Yousafzai et al., 2009; Boateng et al., 2016). From previous studies, trust has a positive influence on the intention to use e-banking (Aladwani, 2001; Febrianto et al., 2018). The intensity of belief positively influences the likelihood of users' usage for subsequent transactions (Bhattacherjee, 2002).

2.5. Relationship between fear of online identity theft, trust, and usage intention

Trust is also placed as a mediating variable in the relationship between fear of online identity theft and the intention to use e-banking in the study of Jibril et al. (2020) and Madawala and Shanika (2021). FOIT has a negative impact on trust in using payment systems (Schreft, 2007), especially in using e-banking (Jibril et al., 2020).

From the result of previous studies, trust is an essential factor in: 1) electronic applications usage (Aladwani, 2001; Rofiq, 2007; Febrianto et al., 2018), 2) e-commerce acceptance in consumers (McKnight et al., 2002; McCole et al., 2010), 3) the adoption process of e-banking (Abu-Shanab & Pearson, 2007; Abu-Shanab et al., 2010). In the research of Boateng et al. (2016) and Jibril et al. (2020), trust has a significant, positive influence on the intention to use e-banking.

Research model is proposed in the Figure 1. Based on review of literature, some hypotheses have been designed in Table 1, below.

Figure 1. Research model proposed

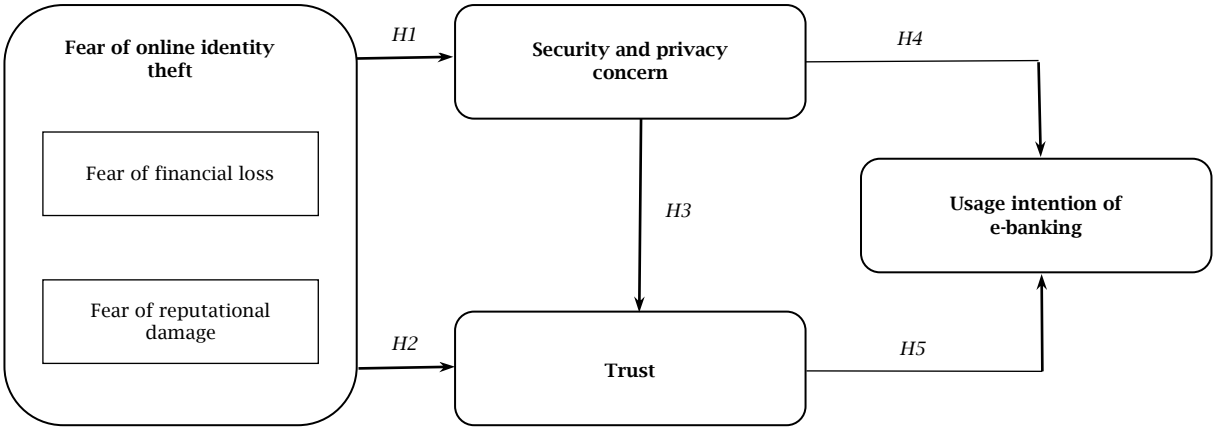

Table 1. Hypotheses

Code	*Hypotheses*	*Sources*
H1	Security and privacy concern (SAPC) positively mediates the relationship between fear of online identity theft (FOIT) and intention in the quest to the usage intention of e-banking (UIEB).	(Jibril et al., 2020)
H2	Trust (T) positively mediates the relationship between fear of online identity theft FOIT and the usage intention of e-banking (UIEB).	New detection
H3	Security and privacy concerns (SAPC) positively affect trust (T) in the quest for the usage intention of e-banking.	New detection
H4	Customer's security and privacy concern (SAPC) negatively affect the usage intention of e-banking (UIEB).	(Jibril et al., 2020)
H5	Customer's trust (T) positively affect the usage intention of e-banking (UIEB).	New detection

Source: Authors' compilation from literature review, 2022.

3. RESEARCH METHODOLOGY

This paper collected data by conducting a quantitative survey using questionnaires developed based on a review of the literature. The result is a total of 441 valid responses from residents in Hanoi, Vietnam, including those who had previously subscribed to e-banking services from several banks or have never interacted with e-banking services. The respondents' answers were entirely voluntary, and convenience sampling technique was performed based on participants' intention to continue using e-banking. The approval for choosing students as research subjects is that many academic researchers have done so (Alsajjan, 2009; Zhao et al., 2010). The study used a five-point Likert scale (1 = "*strongly disagree*"; 5 = "*strongly agree*") to record responses. The research team adapted 27 items from Jibril et al. (2020), Chellappa and Sin (2005), Yousafzai et al. (2009) and developed eight

more items to the questionnaires. The questionnaire includes fear of financial loss (FOFL, five items), fear of reputational damage (FORD, four items), security and privacy concern (SAPC, fourteen items), trust (*T*, five items), usage intention (UIEB, seven items). The structural model was built with variables identified as affecting the intention to participate in using e-banking through the study of reputable selected literature reviews. The suggested hypotheses will be stated at the end of each variable.

The data collected was then used first to measure the reliability using Cronbach's alpha coefficient through SPSS Statistics 23. Following the reliability test, the research team used AMOS 24 to conduct an explanatory factor analysis (EFA) to confirm the validity of each structure and establish representative variables. Finally, the researchers evaluate the established research hypothesis using confirmatory factor analysis (CFA) and the structural equation model (SEM).

4. RESEARCH RESULTS

Receiving 497 responses, 441 of which are valid, this number meets Yamane's (1973) sample size requirement. Out of 441 valid respondents, 279 (63.3%) were female and 161 (36.5%) were male. The respondents were between the ages of under 20 to 55 and have a university education (87.1%). According to Kemp (2022), 16.1% of Vietnam's population is between the ages of under 20 to 25, and 16.7% lies in the age group of 25 to 34. These two age groups have the largest proportion among others and the results received from the survey are appropriate with the population rate of Vietnam in 2022. People in this age group tend to adopt online utility tools more easily, frequently access social network information, and have easier survey access than other age groups. This can show that the objects for the research are well-chosen. The majority of respondents were young and well-educated with the main income range per month being less than 5,000,000 Vietnamese dong (VND) (62.8%). The result shows that 420 people out of 441 are using e-banking services which accounted for 95.2%. This demonstrates how widely used online banking is in Vietnam (see Table 2).

4.1. Reliability test with Cronbach's alpha

The reliability scale for variables is being conducted through Cronbach's alpha. Cronbach's alpha has a bottom limit value of 0.70, which can be reduced to 0.60 for exploratory study, according to Hair et al. (2009). The reliability testing results show that Cronbach alpha's has a value range of 0,771–0.920, which meets the requirements. Among the observed variables, the research team decided to remove two variables *T5* (Factor of trust) and *UIEB1* (factor of usage intention) since their value of correlation are below 0.3 (Nunally & Burnstein, 1994). Cronbach's alpha after adjusting the scale is illustrated in Table 3.

Table 2. Respondents' demographic information

Items	*Number*	*Percentage*
Gender		
Male	161	36.50%
Female	279	63.30%
Prefer not to say	1	0.20%
Total	441	100%
Age		
From under 20 to 20	233	52.80%
From 21 to 25	135	30.60%
From 26 to 40	51	11.60%
From 41 to 55	22	5.00%
Total	441	100%
Academic qualifications		
High school	22	5.00%
College	4	0.90%
University	384	87.10%
Postgraduate	31	7.00%
Total	441	100%
Income per month		
Less than 5,000,000 VND	277	62.80%
From 5,000,000 VND to less than 10,000,000 VND	72	16.30%
From 10,000,000 VND to less than 20,000,000 VND	41	9.30%
From 20,000,000 VND to less than 30,000,000 VND	26	5.90%
From 30,000,000 VND to less than 40,000,000 VND	12	2.70%
From 40,000,000 VND to less than 50,000,000 VND	8	1.80%
More than 50,000,000 VND	5	1.10%
Total	441	100%
The use of e banking		
Yes	420	95.20%
No	21	4.80%
Total	441	100%

Note: VND stands for Vietnamese dong (Vietnamese currency).

Table 3. Result of reliability test

Components	*No. of items before adjusting*	*No. of items after adjusting*	*Cronbach's alpha*	*Corrected item-total correlation*
FOFL	5	5	0.891	0.667–0.773
FORD	4	4	0.920	0.792–0.847
SAPC	14	14	0.920	0.478–0.735
T	4	5	0.771	0.339–0.709
UIEB	6	7	0.808	0.358–0.694

4.2. Exploratory factor analysis

After running the exploratory factor analysis (EFA) test, the Kaiser-Meyer-Olkin (*KMO*) value was met the requirement of $0,5 \leq KMO \leq 1$ (Garson, 2003). The Bartlett's test was significant (Bartlett's test of sphericity) (sig. = 0.000) strengthening the correlation matrix's factorability. Considering the extracted factors, the research team decided to eliminate two observed variables with factor loadings lower than 0.5 (*T1* and *UIEB2*). Also, *UIEB3* with the load factor of 0.505 which is close to the threshold, the research team agree to remove this variable to improve the quality of the scale.

Table 4 shows more latent factors that are separated from the independent variable *SAPC*. The first new sub-factor group includes: 1) *SAPC1*, 2) *SAPC2*, and 3) *SAPC3*. The second sub-factor consists of *SAPC4* to *SAPC14*. Considering the theoretical basis and question content of

the observed variables belonging to Security and Privacy Concern, the author group decided to separate into two new group: 1) Internet security and privacy concern (*SAPCI*) and e-banking security and privacy concern (*SAPCE).*

Table 4. Result of factor loading, KMO and eigenvalues of independent variables

Components	*No. of items*	*Factor loading*	*KMO*	*Eigenvalues*
FOFL	5	0.610–0.750	0.869	3.509
FORD	4	0.883–0.917	0.849	3.226
SAPCE	11	0.601–0.795	0.916	7.980
SAPCI	3	0.792–0.808	0.916	1.292
T	3	0.799–0.808	0.916	2.575
UIEB	4	0.712–0.827	0.916	1.737

Because the variable security and privacy concern has been split into two new variables, some new hypotheses are designed as below:

H1a: SAPCI mediates the relationship between FOIT and UIEB.

H1b: SAPCE mediates the relationship between FOIT and UIEB.

H3a: SAPCI affects trust in the quest for the usage intention of e-banking.

H3b: SAPCE affects trust in the quest for the usage intention of e-banking.

H4a: Customer's security and privacy concern about Internet (SAPCI) negatively affect the usage intention of e-banking (UIEB).

H4b: Customer's security and privacy concern about e-banking (SAPCE) negatively influence the usage intention of e-banking (UIEB).

4.3. Confirmatory factor analysis

The fit of the model (*Model Fit*) is calculated through confirmatory factor analysis (CFA) and the results states a great model with the results shown in Table 5 below:

Table 5. Confirmatory factor analysis

Measure	*Results*	*Threshold*	*Sources*
CMIN/df	2.518	Good (≤ 3)	Hair et al. (2009)
Comparative fit index (CFI)	0.926	Good (≥ 0.9)	Hair et al. (2009)
Goodness of fit index (GFI)	0.863	Acceptable (≥ 0.8)	Baumgartner and Homburg (1995)
Tucker Lewis index (TLI)	0.918	Good (≥ 0.9)	Hu and Bentler (1999)
Root mean squared error of approximation (RMSEA)	0.059	Good (≤ 0.08)	Hair et al. (2009)

CFA continues to consider the convergent validity and discriminant validity between groups of variables. Hair et al. (2009) found that the factor loading of all items was more than 0.5. Furthermore, the average variance extracted (AVE) for each construct is greater than 0.5, and the construct reliability (CR) for all latent variables is greater than 0.7. All of the indicators had sufficient loading and were appropriate. The discriminant validity of a latent component was assessed by comparing its square root of AVE (SQRTAVE) to all constructed correlations. Through all the measures that have been made, we found that the SQRTAVE of the FOFL variable is greater than the absolute value of the Inter-construct correlations. After considering, the research team decided to remove the observed variable *FOFL4*. The final model validity test results are obtained in Table 6, below:

Table 6. Discriminant and correlations among the constructs

Components	*CR*	*AVE*	*MSV*	*MaxR(H)*	*SAPCE*	*UIEB*	*T*	*SAPCI*	*FOFL*	*FORD*
SAPCE	0.926	0.533	0.308	0.929	0.730					
UIEB	0.818	0.530	0.220	0.827	0.322***	0.728				
T	0.853	0.659	0.270	0.854	0.520***	0.469***	0.812			
SAPCI	0.797	0.567	0.349	0.799	0.555***	0.173**	0.156**	0.753		
FOFL	0.887	0.662	0.617	0.889	0.450***	0.243***	0.365***	0.531***	0.814	
FORD	0.920	0.743	0.617	0.922	0.416***	0.267***	0.397***	0.590***	0.785***	0.862

*Note: Significance of correlations — p < 0.100, * p < 0.050, ** p < 0.010, *** p < 0.001.*

Thus, the CFA results have shown that the hypothesis model suggested by the authors is theoretically suitable.

4.4. Structural equation model (SEM) analysis

Figure 2 illustrates shows that the theoretical model has a model fit Chi-square = 953.241, Chi-square/df = 2,590; *GFI* = 0.865; *CFI* = 0.924 and *RMSEA* = 0.060 were both satisfactory and accepted (Schumacker & Lomax, 2004).

Most of the standardized regression weights have a positive index showing the degree of positive impact of the independent variables on the dependent variable. Only the standardized regression weights of the *SAPCI* effect on *T* has negative values, which shows the negative impact of the *SPACI* variable on the variable *T*. The result also shows that the *p*-value for the effect of *SAPCI* and *SAPCE* to the *UIEB* are greater than 0.05, so these two hypotheses are being rejected (see Table 7).

Figure 2. SEM results

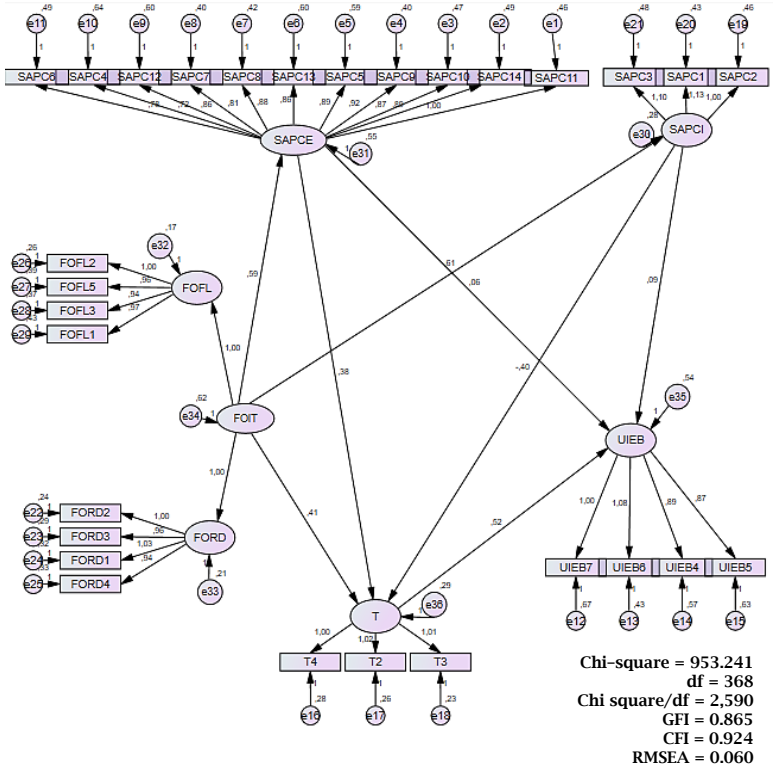

Table 7. The result summary

Hypotheses	*Path*			*Description*	*Estimate*	*SE*	*CR*	*p-value*	*Outcome*
H1a	FOIT	⟶	SAPCI	SAPCI mediates the relationship between FOIT and UIEB.	0.611	0.055	11.079	***	Supported
H1b	FOIT	⟶	SAPCE	SAPCE mediates the relationship between FOIT and UIEB.	0.590	0.059	9.944	***	Supported
H2	FOIT	⟶	T	Trust mediates the relationship between FOIT and UIEB.	0.414	0.079	5.247	***	Supported
H3b	SAPCE	⟶	T	SAPCE affect Trust.	0.376	0.049	7.746	***	Supported
H3a	SAPCI	⟶	T	SAPCI affect Trust.	-0.400	0.080	-5.015	***	Supported
H5	T	⟶	UIEB	Trust affects UIEB.	0.516	0.085	6.100	***	Supported
H4a	SAPCI	⟶	UIEB	SAPCI affect UIEB.	0.093	0.069	1.348	0.178	Rejected
H4b	SAPCE	⟶	UIEB	SAPCE affect UIEB.	0.058	0.067	0.860	0.390	Rejected

*Note: *** p < 0.001.*

5. DISCUSSION

According to the survey, the respondents' frequency in using e-banking before being influenced by uncertain contexts is different compared to the data collected after they have experienced an aforementioned situation. After the occurrence of uncertain context, 9% of the "*Mostly all the time*" answers were added by the respondents, indicating that they tend to use e-banking more often than before. Due to COVID-19, more consumers are choosing to work from home in order to prioritize saving overspending, and operate business online (Bytyçi et al., 2021). The research participants who did not use e-banking (3.21%) or rarely use it (22.3%), started using the service more frequently after experiencing uncertainty which could highly affected their discretion in sharing personal information. Most of the responders (86.7%) are positive about the impact of the stated contexts to their behavior of being cautious about sharing personal information online, whereas the remaining answerers (13.3%) are less vulnerable to those situations. The percentage of users that make use of the service most of the time has increased to roughly 5% when compared to before the era of unpredictability. The Internet and technology advances promote incremental changes in customers' routines and behaviors. In addition, banks leverage changing user preferences to their advantage, greatly enhancing the functionality and quality of e-banking systems (such as *VietcomBank*, *VietinBank*, *BIDV*, etc.). This study clarifies the existing consensus about online identity theft in Hanoi by considering the realities of a rising economy, particularly in an uncertain situation. The study equation's findings indicate that the determinants employed are accurate and trustworthy, additionally, the model's structure is regarded as suitable.

5.1. The effect of fear of online identity theft on security and privacy concerns

Many banks now provide "*full service*" internet banking, which includes online bill payment as well as lending and brokerage services. An increasingly

skilled high-tech criminal has emerged as a result of the fast evolution of technology. Customers' desires, frequent use, and flaws in bank intermediary transactions have all been used by identity thieves to conduct fraud. One of the main causes for which our research participants are more cautious when disclosing personal information is due to this situation. If users are aware that theft is a possibility and that it might have negative effects, they will view it as technological harm and take precautions. Our research team found out that customers believe identity theft may happen during e-banking transactions, which is in line with studies from (Fernandes et al., 2014; Walsh et al., in press). Besides, our study shows how this validates the perceived risk of online identity theft. In particular, *FOIT* and *SAPC* have a direct correlation, and the *SAPC* variable, which has two sub-factors called *SAPCE* and *SAPCI*, contains new findings. E-banking customers commonly experience anxiety while doing transactions with other parties, such as when they suspect their data and money may have been stolen from the third party.

5.2. The effect of security and privacy concerns on trust

One of the two new-finding variables, *SAPCI*, has a negative impact on the *Trust* variable, whereas *SAPCE* has a positive impact. People who accept new technology are said to do out of a sense of confidence (Gefen et al., 2003). In order for customers to trust the objective of utilizing e-banking, they must be convinced that the transactional medium is secure and that any information they provide to those websites is not being confiscated or transferred to a third party (Suh & Han, 2003). The nature of service delivery online is produced by the lack of direct physical interaction, much as how client adoption of online banking is hindered by a lack of trust (Chaouali et al., 2016; Yousafzai et al., 2009). People still have security concerns with regard to Internet regulation and are concerned about information theft.

5.3. The effect of security and privacy concerns on usage intention of e-banking

Additionally, the two variables (*SAPCI* and *SAPCE*) in the current study show no positive or direct relationships with *UIEB*. As an explanation for our recent research, we surmise that because e-banking was widely used during the COVID-19 epidemic and individuals under quarantine had no other choice than to use it, Hanoians continued to use it after COVID-19. Although consumers have privacy and security concerns, the results suggest that the percentage of information stolen on internet platforms was minimal (19% of respondents). Due to the development of modern technology and the Internet, clients in Vietnam can access E-commerce through internet banking, and e-banking services are being developed in a more secure manner to meet the trend of using the bank's services. As a result, their trust in banks is also high. The perceived level of risk in various types of transaction is uncertain, despite the actual risk of third parties getting personal information or financial data online is lower than through more traditional means (Miyazaki & Fernandez, 2001). The Internet is far safer than conventional mail or phone order arrangements because of the number of security features, such as encryption. Therefore, the theory is disproved since this internet-related issue barely affects intention.

5.4. The effect of trust on usage intention of e-banking and the effect of fear of online identity theft on trust

Trust is viewed as a key element of internet banking due to the "*spatial and temporal isolation*" between the customer and the bank (Grabner-Kraeuter, 2002). Customer encounters and perceptions of service qualities, including the veracity of the information, the usability of the website, the privacy of information sharing, and the efficiency of transaction execution have an impact on trust in the e-banking environment (Balasubramanian et al., 2002). Consumers, whether adopters or non-adopters, believe that they are particularly concerned about accessibility and anonymity in internet banking (Gerrard & Barton Cunningham, 2003). Additionally, trust is viewed as a motivator in many transactions that might help clients establish long-lasting business relationships (Hawes et al., 1989). This is the rationale behind the findings, which show how trust *(T)* positively influences the *UIEB*. The research suggests that removing uncertainty is crucial to ensure that customers adopt online banking. Customers may only benefit from *trust's* significant effects if they have confidence in the bank's ongoing willingness and ability to uphold its part of the contract. This assurance is based on three things: confidence in the bank, assurance in the security features integrated into the website, and confidence that customers' transaction data will not be used without their permission (perceived privacy) (Yousafzai et al., 2009). The respondents to the research also exhibit a positive association between their trust *(T)* and this perceived cue (*FOIT*). Perceived identity theft is one of the numerous guises that cyber-security dangers can take. This occurs when a customer lacks confidence in transactions and worries that a third party could steal their personal information (such as name, address, phone number, etc.) when they make a buy or a sale from any related e-business. This is due to the rise in identity theft cases brought on by the expansion of online business transactions, which has led to enormous costs for both consumers and the e-commerce industry.

6. CONCLUSION

This is one of the first studies done in Vietnam to look at how online identity theft affects people's desire to utilize e-banking services. According to research findings, security and privacy concerns are positively impacted by fear of online identity theft. When people are cautious about revealing their personal information when utilizing e-banking services, it's generally because they are aware of cybercrime and fear online identity theft. With e-banking, this took place in the opposite manner. Customers always have some level of confidence in the banking system because of excellent rules and

financial education programs that teach people about the financial sector in general and personal information security in particular. This is further demonstrated by the study's findings, which show that trust is positively impacted by fear of online identity theft. Customers frequently seek detailed information about security and privacy from a number of sources, including: 1) the Internet, 2) bank tellers, and 3) published papers because they are concerned about personal information being stolen. Additionally, we discovered that trust had a favorable impact on usage intention of e-banking. Customers are more inclined to utilize the goods and services when they think the bank's policies and regulations will maintain their legitimacy and dependability, as is clear. The study is expected to provide further insight into how strategically digital technologies are being accepted and used in business and society, particularly in the banking sector of the banking industry. Because of this, it is hoped that this study will serve as a framework for future scholars to utilize as the basis for their quantitative research into the phenomenon of consumers' constraints toward online banking activity and other pertinent themes. Furthermore, the challenges that customers have while selecting whether to make an online banking transaction in Hanoi's unpredictable environment will be addressed by this research's assistance to financial sector regulators and bankers.

Some limitations, nevertheless, still need to be addressed since they provide room for more research. Only 441 of the sample's 497 responses were initially authorized. It's also challenging to conceive employing intentions with people of greater rank given the wide income divide between men and women. This problem is further exacerbated by the fact that the study exclusively used the student population, making it difficult to generalize outside the target group.

This paper also makes some recommendations for practical solutions for prospective clients, banks, and policymakers. Commercial banks should re-establish security procedures and encrypt consumer transaction information to improve dependability and keep potential customers. Banks should also reexamine the problem of confirming the legitimacy of consumers while conducting transactions. There are three methods to verify a client's identification, according to: 1) what the customer knows (password, PIN code), 2) the customer possesses (bank chip card, hardware device), and 3) the customer represents (fingerprint, iris, retina scan) (Parusheva, 2009). To improve the security of customer transaction information, banking systems must upgrade their multi-factor authentication procedures. Bank should also invest in IT cyber security and work with third-party firms to implement safety methods such as employee training courses, identify gaps in current cyber policies, and provide risk-relief products such as cyber insurance (Hogan, 2020). For clients, the best action for consumers to prevent theft is to avoid clicking on suspicious links, not to disclose personal information to random people, and to use passwords with high levels of protection. The major goal is to prevent users' personal information from being leaked, and this is also seen as the first step in protecting users' data and accounts because it's likely that criminals may discover them and try to use their identities without acknowledgement. Policymakers should establish a fundamental and more stringent general legal framework on this issue, and clarify and review privacy responsibilities information on deposits, accounts, transactions of customers, and deposited assets at credit institutions, as well as foreign bank branches. This will help policymakers develop a setting that supports secure e-banking services and the security of financial customers. To prevent crime and safeguard users' rights and interests, competent authorities may enact harsher laws and punishments.

REFERENCES

1. Abu-Shanab, E., & Pearson, J. M. (2007). Internet banking in Jordan: The unified theory of acceptance and use of technology (UTAUT) perspective. *Journal of Systems and Information Technology, 9*(1), 78–97. https://doi.org/10.1108/13287260710817700
2. Abu-Shanab, E., Pearson, J., & Setterstrom, A. (2010). Internet banking and customers' acceptance in Jordan: The unified model's perspective. *Communications of the Association for Information Systems (CAIS), 26*(23), 493–525. https://doi.org/10.17705/1CAIS.02623
3. Ajide, F. M. (2016). Financial innovation and sustainable development in selected countries in West Africa. *Journal of Entrepreneurship, Management and Innovation, 12*(3), 85–111. https://doi.org/10.7341/20161234
4. Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T
5. Al-Smadi, M. O. (2012). Factors affecting adoption of electronic banking: An analysis of the perspectives of banks' customers. *International Journal of Business and Social Science, 3*(17), 294–309. http://ijbssnet.com/view.php?u=https://ijbssnet.com/journals/Vol_3_No_17_September_2012/33.pdf
6. Aladwani, A. M. (2001). Online banking: A field study of drivers, development challenges, and expectations. *International Journal of Information Management, 21*(3), 213–225. https://doi.org/10.1016/S0268-4012(01)00011-1
7. Alsajjan, B. (2009). The relative importance of trust intentions and trust beliefs in internet banking adoption. *International Review of Business Research Papers, 5*(6), 231–247. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=8487e5ee28f3d4141491eb0b92d956c6085cbec4
8. Alkrisheh, M. A. (2022). Criminal protection of corporate websites: An analytical study. *Journal of Governance & Regulation, 11*(3), 148–154. https://doi.org/10.22495/jgrv11i3art12
9. Amoroso, D. L., & Hunsinger, D. S. (2009). Understanding consumers' acceptance of online purchasing. *Journal of Information Technology Management, 10*(1), 15–41. https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=4162&context=facpubs

10. Balasubramanian, S., Peterson, R. A., & Jarvenpaa, S. L. (2002). Exploring the implications of m-commerce for markets and marketing. *Journal of the Academy of Marketing Science, 30*, 348–361. https://doi.org/10.1177/009207002236910
11. Berghel, H. (2000). Identity theft, social security numbers, and the web. *Communications of the ACM, 43*(2), 17–21. https://doi.org/10.1145/328236.328114
12. Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *The Journal of Strategic Information Systems, 11*(3–4), 245–270. https://doi.org/10.1016/S0963-8687(02)00018-5
13. Bhattacherjee, A. (2002). Individual trust in online firms: Scale development and initial test. *Journal of Management Information Systems, 19*(1), 211–241. https://doi.org/10.1080/07421222.2002.11045715
14. 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
15. Bytyçi, S., Shala, V., Ziberi, B., & Myftaraj, E. (2021). Transforming traditional business into online: The impact of COVID-19 pandemic on consumer behavior. *Journal of Governance & Regulation, 10*(2), 300–308. https://doi.org/10.22495/jgrv10i2siart10
16. Castañeda, J. A., & Montoro, F. J. (2007). The effect of internet general privacy concern on customer behavior. *Electronic Commerce Research, 7*, 117–141. https://doi.org/10.1007/s10660-007-9000-y
17. Chaouali, W., Yahia, I. B., & Souiden, N. (2016). The interplay of counter-conformity motivation, social influence, and trust in customers' intention to adopt Internet banking services: The case of an emerging country. *Journal of Retailing and Consumer Services, 28*, 209–218. https://doi.org/10.1016/j.jretconser.2015.10.007
18. Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management, 6*(2–3), 181–202. https://doi.org/10.1007/s10799-005-5879-y
19. Clay, K., & Strauss, R. (2000). Trust, risk and electronic commerce: Nineteenth century lessons for the twenty-first century. *Proceedings of the Annual Conference on Taxation and Minutes of the Annual Meeting of the National Tax Association, 93*, 53–63. http://www.jstor.org/stable/41950586
20. Cornelius, D. R. (2016). *Online identity theft victimization: An assessment of victims and non-victims level of cyber security knowledge* [Doctoral dissertation, Colorado Technical University]. ProQuest Dissertations & Theses Global.
21. Kemp, S. (2022, February 15). *Digital 2022: Vietnam.* DataReportal. https://datareportal.com/reports/digital-2022-vietnam
22. Sepashvili, E. (2020). Digital chain of contemporary global economy: E-commerce through e-banking and e-signature. *Economia Aziendale Online, 11*(3), 239–249. http://doi.org/10.13132/2038-5498/11.3.239-249
23. Febrianto, G., Hidayatullah, S., & Ardianto, Y. T. (2018). The effect of intention to usage to actual usage e-purchasing application. *International Journal of Scientific & Engineering Research, 9*(12), 363–370. http://surl.li/jmpfg
24. Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M., & Inácio, P. R. (2014). A quick perspective on the current state in cybersecurity. In B. Akhgar & H. R. Arabnia (Eds.), *Emerging trends in ICT security*: *Emerging trends in computer science and applied computing* (1st ed., pp. 423–442). Morgan Kaufmann. https://doi.org/10.1016/b978-0-12-411474-6.00025-6
25. Forsythe, S., Liu, C., Shannon, D., & Gardner, L. C. (2006). Development of a scale to measure the perceived benefits and risks of online shopping. *Journal of Interactive Marketing, 20*(2), 55–75. https://doi.org/10.1002/dir.20061
26. Garson, G. D. (Ed.). (2003). *Public information technology: Policy and management issues.* IGI Global. https://doi.org/10.4018/978-1-59140-060-8
27. Grabner-Kraeuter, S. (2002). The role of consumers' trust in online-shopping. *Journal of Business Ethics, 39*, 43–50. https://doi.org/10.1023/A:1016323815802
28. Gefen, D. (2000). E-commerce: The role of familiarity and trust. *Omega, 28*(6), 725–737. https://doi.org/10.1016/s0305-0483(00)00021-9
29. Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51–90. https://doi.org/10.2307/30036519
30. Gerrard, P., & Barton Cunningham, J. (2003). The diffusion of Internet banking among Singapore consumers. *International Journal of Bank Marketing, 21*(1), 16–28. https://doi.org/10.1108/02652320310457776
31. Gurung, A., & Raja, M. K. (2016). Online privacy and security concerns of consumers. *Information and Computer Security, 24*(4), 348–371. https://doi.org/10.1108/ics-05-2015-0020
32. Hair, J. F. (2009). *Multivariate data analysis.* DIGITALCOMMONS.Kennesaw State University.
33. Hawes, J. M., Mast, K. E., Swan, J. E. (1989). Trust earning perceptions of sellers and buyers. *Journal of Personal Selling & Sales Management*, *9*, 1–8. http://surl.li/joaie
34. Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing, 30*(1), 1–19. https://doi.org/10.1016/j.intmar.2014.10.001
35. Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM, 42*(4), 80–85. https://doi.org/10.1145/299157.299175
36. Hogan, K. M. (2020). A global comparison of corporate value adjustments to news of cyber-attacks. *Journal of Governance & Regulation, 9*(2), 34–44. http://doi.org/10.22495/jgrv9i2art2
37. Homburg, C., & Baumgartner, H. (1995). Beurteilung von Kausalmodellen: Bestandsaufnahme und Anwendungsempfehlungen [Assessment of causal models: Inventory and recommendations for use]. *Marketing: Zeitschrift Für Forschung Und Praxis, 17*(3), 162–176. https://doi.org/10.15358/0344-1369-1995-3-162
38. Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal, 6*(1), 1–55. http://doi.org/10.1080/10705519909540118

39. Jibril, A. B., Kwarteng, M. A., Botchway, R. K., Bode, J., & Chovancova, M. (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), Article 1832825. https://doi.org/10.1080/23311975.2020.1832825
40. Jogiyanto, H. M. (2007). *Sistem informasi keperilakuan* [Behaviour information system]. Yogyakarta: Andi Offset.
41. 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
42. Lafraxo, Y., Hadri, F., Amhal, H., & Rossafi, A. (2018). The effect of trust, perceived risk and security on the adoption of mobile banking in Morocco. In *Proceedings of the 20th International Conference on Enterprise Information Systems (ICEIS 2018).* https://doi.org/10.5220/0006675604970502
43. 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
44. Lin, F., Wu, H., & Tran, T. N. (2014). Internet banking adoption in a developing country: An empirical study in Vietnam. *Information Systems and E-Business Management, 13*, 267–287. https://doi.org/10.1007/s10257-014-0268-x
45. Maditinos, D., Chatzoudes, D., & Sarigiannidis, L. (2013). An examination of the critical factors affecting consumer acceptance of online banking: A focus on the dimensions of risk. *Journal of Systems and Information Technology, 15*(1), 97–116. https://doi.org/doi:10.1108/13287261311322602
46. Madawala, S., & Shanika, S. (2021). Fear of online identity theft on online purchase intention in a Sri Lankan context: Mediating role of trust in e-payment systems. *Proceedings of the 3rd Commerce Research Symposium 2021.*
47. McCole, P., Ramsey, E., & Williams, J. (2010). Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns. *Journal of Business Research, 63*(9–10), 1018–1024. https://doi.org/10.1016/j.jbusres.2009.02.025
48. McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13*(3), 334–359. https://doi.org/10.1287/isre.13.3.334.81
49. 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
50. Mori, N., & Mlambiti, R. (2020). Determinants of customers' adoption of mobile banking in Tanzania: Further evidence from a diffusion of innovation theory. *Journal of Entrepreneurship, Management and Innovation, 16*(2), 202–230. https://doi.org/10.7341/20201627
51. Nunally, J. C., & Bernstein, I. H. (1994). *Psychology theory* (3rd. ed.). McGrew-Hill.
52. 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. In *Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020.* Academic Conferences and Publishing Limited. http://surl.li/jmvmq
53. Parusheva, S. (2009). Identity theft and internet banking protection. *Economic Alternatives, 1*, 44–55. https://www.unwe.bg/uploads/Alternatives/A05_01.2009.pdf
54. 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, 50*(2), 216–238. https://doi.org/10.1177/0022427811425539
55. Ratnasingam, P., Pavlou, P. A., & Tan, Y. H. (2002, June 17–19). The importance of technology trust for B2B electronic commerce. In *Proceedings of the 15th Bled Electronic Commerce Conference eReality: Constructing the eEconomy* (pp. 384–398). Bled, Slovenia. http://surl.li/jmwjk
56. Reyns, B. W., & Henson, B. (2015). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy and Comparative Criminology, 60*(10), 1119–1139. https://doi.org/10.1177/0306624x15572861
57. Rofiq, A. (2007). *Pengaruh dimensi kepercayaan (Trust) terhadap partisipasi pelanggan E-commerce* [The influence of trust dimensions on e-commerce customer participation] [Master's thesis, Universitas Brawijaya Malang]. Universitas Brawijaya Malang. http://surl.li/jmwwf
58. Sathye, M. (1999). Adoption of internet banking by Australian consumers: An empirical investigation. *International Journal of Bank Marketing, 17*(7), 324–334. https://doi.org/10.1108/02652329910305689
59. Schreft, S. L. (2007). Risks of identity theft: Can the market protect the payment system? *Federal Reserve Bank of Kansas City Economic Review, 92*(Q4), 5–40. http://surl.li/jmxdd
60. Shannak, R. O. (2013). Key issues in e-banking strengths and weaknesses: The case of two Jordanian banks. *European Scientific Journal, 9*(7), 239–263. https://core.ac.uk/download/pdf/328023566.pdf
61. Schumacker, R. E., & Lomax, R. G. (2004). *A beginner's guide to structural equation modeling: Fourth edition* (2nd. ed.). Psychology Press. https://doi.org/10.4324/9781410610904
62. Smith, R., Roberts, L., Biles, D., & Thorne, C. (2007). Reviews. *Australian & New Zealand Journal of Criminology, 40*(3), 360–370. https://doi.org/10.1375/acri.40.3.360
63. Suh, B., & Han, I. (2003). The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of Electronic Commerce, 7*(3), 135–161. https://doi.org/10.1080/10864415.2003.11044270
64. Tam, L. T., Chau, N. M., Mai, P. N., Phuong, N. H., & Tran, V. K. H. (2020). Cyber crimes in the banking sector: Case study of Vietnam. *International Journal of Social Science and Economics Invention, 6*(5), 272–277. https://doi.org/10.23958/ijssei/vol06-i05/207
65. Ting, H., Yacob, Y., Liew, L., & Lau, W. M. (2016). Intention to use mobile payment system: A case of developing market by ethnicity. *Procedia — Social and Behavioral Sciences, 224*, 368–375. https://doi.org/10.1016/j.sbspro.2016.05.390
66. Udo, G. J. (2001). Privacy and security concerns as major barriers for e-commerce: A survey study. *Information Management & Computer Security, 9*(4), 165–174. https://doi.org/10.1108/EUM0000000005808
67. van der Meulen, N. (2006). *The challenge of countering identity theft: Recent developments in the United States, the United Kingdom, and the European Union* (Report). National Infrastructure Cyber Crime program (NICC). https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=7dddefbe7a6751f11fe0e8baf66a982d69999035

68. Vasileiadis, A. (2014). Security concerns and trust in the adoption of m-commerce. *Social Technologies, 4*(1), 179–191. https://doi.org/10.13165/st-14-4-1-12
69. Venkatesh, V. (2000). Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information Systems Research, 11*(4), 342–365. https://doi.org/10.2139/ssrn.4062395
70. Walsh, G., Hille, P., & Cleveland, M. (in press). Fearing online identity theft: A segmentation study of online customers. *Association for Information Systems AIS Electronic Library (AISeL).* https://core.ac.uk/download/pdf/301369874.pdf
71. Wang, Y.-S., Wang, Y.-M., Lin, H.-H., & Tang, T.-I. (2003). Determinants of user acceptance of internet banking: An empirical study. *International Journal of Service Industry Management, 14*(5), 501–519. https://doi.org/10.1108/09564230310500192
72. Yamane, T. (1973). *Research methodology/Sample size.* University of Florida.
73. Yamane, T. (1973). *Statistics. An introductory analysis* (3rd. ed.). Harper & Row.
74. Yousafzai, S., Pallister, J., & Foxall, G. (2009). Multi-dimensional role of trust in internet banking adoption. *The Service Industries Journal, 29*(5), 591–605. https://doi.org/10.1080/02642060902719958
75. Zhao, A., Koenig-Lewis, N., Hanmer-Lloyd, S., & Ward, P. (2010). Adoption of internet banking services in China: Is it all about trust? *International Journal of Bank Marketing, 28*(1), 7–26. https://doi.org/10.1108/02652321011013562