International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 02, 2020
ISSN: 1475-7192

The Sufficiency of the "Contactless Cards" Security Features in Preventing Fraud-A Malaysian Study

[1]Mansourah Banon Hosany, [2]Geetha A. Rubasundram

Abstract--*Contactless Cards are a revolutionary innovation in transaction payments. Little is known; however, about what shapes end users' willingness and perception to use this method. The objective of this study is to compare the end-users and banks perceptionon the sufficiency of contactless cards. This research will use Fraud Diamond Theory, General Deterrence Theoryand Technology Acceptance Model (TAM) to meet the objective of this study. This research aims to provide a more in-depth analysis; hence a mixed method has been used. The quantitative data was collected from 192 users via questionnaires in Malaysia to be able to evaluate the end user perspective of contactless cards. The results were then analysed via the Statistical Package of the Social Sciences (SPSS). This were then used to gauge the perspective of banks using interviews to analyse key security mechanism for the most popular type of fraud including the relay attacks, electronic pickpocketing, theft and cloning through devices readily available on dark web. The findings of this research suggested that almost 80% of end users of contactless cards were unaware of the types of risks and security features of contactless cards. The interviews reflected that relay attacks are the most prominent risk and that the security measures in place were insufficient. Henceforth, this research recommends that banks need to have more effective awareness programs to educate the users of contactless cards of the risks and security features.*

Key words--*Contactless cards, Perceived Risk, Relay Attacks, Cloning, Dark Web*

I. INTRODUCTION

Modes of payments have developed from the barter system to fiat money and to debit and credit cards, with the growth in financial technologies (Fintech) skyrocketing after 2008. "Fintech" relates to firms and financial institutions that combine financial services with modern and innovative technologies(Dorfleitner, 2017).Being the prominent financial intermediator, banks use Fintech to enhance its payment solutions within the industry. A key Fintech application is contactless cards that increases convenience and reduce fraudulent activities associated with normal debit and credit cards(Deloitte, 2008).Contactless cards allows consumers to pay for a product by simply waving it on an active NFC terminal within 4 to 10 centimetres from the retailer's card reader(Raza, 2016). These cards can be used in tap and go payment terminals normally found in supermarkets, public transports, restaurants,

[1]*Research Scholar, Asia Pacific University, Jalan Teknologi 5,57000 Wilayah Persekutuan Kuala Lumpur, Malaysia. hosanymansourah@gmail.com*
[2] *Senior Lecturer, Asia Pacific University, Malaysia, Jalan Teknologi 557000 Wilayah Persekutuan Kuala Lumpur, Malaysia. geetha@apu.edu.my*

DOI: 10.37200/IJPR/V24I2/PR200413
Received: 19 Dec 2019 | Revised: 04 Jan 2020 | Accepted: 15 Jan 2020

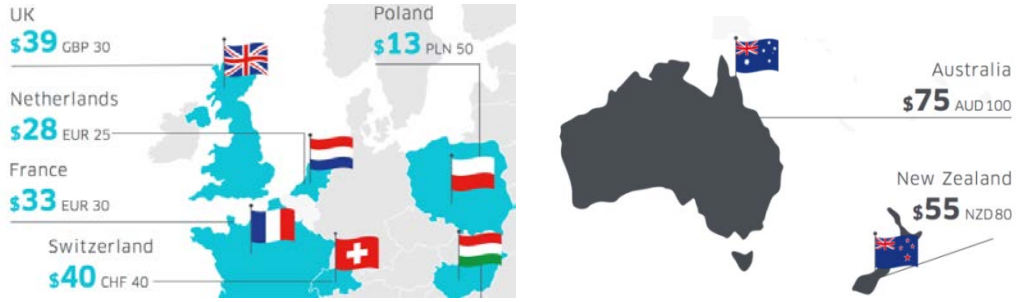
vending machines and many others. Typical examples of contactless cards are Express Pay, Mastercard Paypass, Visa Paywave and Quickpass. The first contactless cards were issued by Barclaycard in 2007 in UK and since then the use of contactless cards spread out to all corners of the world with more than 10 million of contactless cards in circulation. Contactless card contains a RFID symbol as shown in Figure 1.

Figure 1. 1:RFID Symbol

Source: Visa Contactless Card 2018

These cards provide a lot of advantages for its users. Since fiat money is not required, the card reduces queuing time and the risk of being robbed. However, it is vulnerable to other fraudulent activities. Hence, issuers of contactless cards have set certain limits that customers can use to purchase their goods and services, and this varies in each country as shown in Figure 1.2.

European countries **Australasia**



Asian Countries **North America**

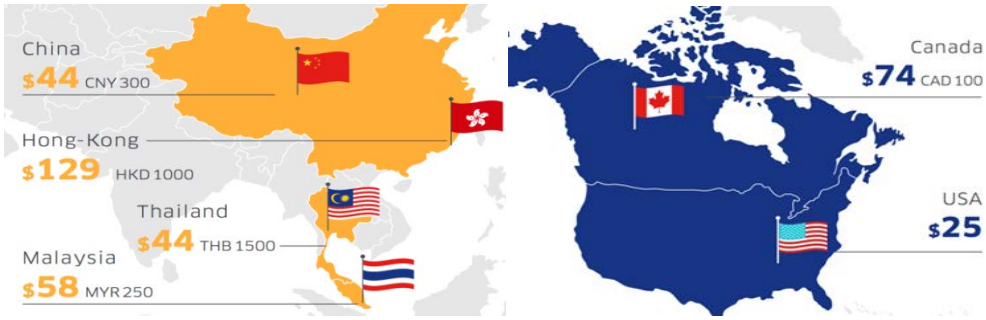


Figure 1. 2 Contactless Cards limits

Source: Ingenico Group 2017

DOI: 10.37200/IJPR/V24I2/PR200413
Received: 19 Dec 2019 | Revised: 04 Jan 2020 | Accepted: 15 Jan 2020

Regardless of the limits set, some customers are not willing to use contactless cards due to risk associated to the different types of frauds such as relay attack, electronic pickpocketing and cloning. Relay attack is a technique where the criminal can intercept, change and manipulate any transaction in real time. Another fraud associated with contactless cards is electronic pick pocketing which occurs when criminals use handheld card readers to skim payment details and sensitive information without the victim noticing or realising(Eccles, 2016). In a shopping mall in Texas, a fraudster was able to charge users Visa Pay wave cards using a falsified payment terminal(Storm, 2013).

In addition, cloning of contactless cards have become very popular. Linked to the Dark Web, the cloning and trading of stolen contactless card information (Simpson, 2016; Cimpanu 2016) has increased especially due to the anonymity of the Dark Web and the skill set of online hackers who can easily change the IP address. An example of the device is Contactless Infusion X5 which was being sold at 1.2 Bitcoin on the Dark Web to copy information from contactless cards and clone(Cimpanu, 2016).

To combat those frauds, banks and regulators have set in place several security mechanisms. One of them is the two-way authentication process which requires two types of credentials for authentication and is designed by banking institutions to reduce a breach in security. Secondly, through the use of Artificial Intelligence (AI), it helps in increasing the reliability of the approval process and in detecting any unusual usage behaviour of the cards. Moreover, RFID wallets is a protection against theft of cards and electronic pickpocketing where it prevents the RFID technology from reaching inside the wallet. Another security feature for contactless cards is the EMV chip which is embedded in the card and generate a valid cryptographic code that is sent back to the payment terminal which proves that the card is genuine.

Regardless of the uncertainty, the increasing usage of the cards is noted. Malaysia is among the countries where contactless cards has risen by 142% to RM1.33 billion in 2016, from RM547.2 million in 2015(Lee & Souza, 2018). Based on Mastercard reports in 2017, this showed that contactless transactions account for 15% of all global transactions at point-of-sale (POS) and within 5 years it is expected to grow up to 53%(Focus Malaysia, 2018). The main banks offering contactless cards in Malaysia are Maybank, CIMB, HSBC Amanah, Citi banks and many others. Although Malaysia has not encountered any contactless card fraud, concerns over the safety issues is still there mainly due to an online video demonstrating the ability of fraudsters to read a cardholder’s personal information from a Visa Pay wave enabled card. However, Bank Negara Malaysia had denied that contactless cards are susceptible to frauds due to the implementation of the two-factor authentication process between the card and the POS terminal which Malaysia adopted. However, it was noted that Union of Bank Employees had warned that no guarantee had been provided to protect the contactless card user from data theft (Daily Express,2016). This have raised a lot of doubts on the perception of the users regarding contactless cards. Nevertheless, the ability for the fraudsters to get access to the personal data of customers indicates that the banks have poor internal control and safeguarding measures. This also hinders that customers do not take the necessary measures when performing any type of contactless transactions.

The above clearly reflects the gap between the perspective of the banks and end users. Applying the gap to a Malaysian perspective, this study will analyse the 3 main factors (usage behaviour, types of frauds and security

DOI: 10.37200/IJPR/V24I2/PR200413
Received: 19 Dec 2019 | Revised: 04 Jan 2020 | Accepted: 15 Jan 2020

features of contactless card) that impact the end user' perception on risks followed by a proper assessment from the banks' perspective on the sufficiency of contactless cards security mechanisms. The researcher will then evaluate the key major differences between the two groups regarding the sufficiency of the security mechanisms such as two-way authentication process, AI, zero liability policy, RFID wallet and cryptography enough to prevent frauds such as relay attacks, electronic pickpocketing, cloning via dark web and theft of contactless cards. Therefore, the ultimate objective of this research is to compare the perspectives of banks and end-users on the sufficiency of the contactless cards' security features in preventing fraud especially since previous studies on contactless cards from the end users and banks perspective have provided mixed conclusions.

II. LITERATURE REVIEW

The use of contactless card is increasing internationally. To assess the susceptibility of users towards contactless cards, this study refers to the Technology Acceptance Model (TAM) framework to predict the users' acceptance of technology. Apart from the initial two factors of perceived usefulness and ease of use, studies by Shin & Lee (2014), Wang (2008), Zheng et al (2013) and Harper (2014) included perceived risk. This is relevant to this study since users would be confronted by various types of contactless cards frauds.

Contactless card fraud is also increasing internationally due to the vulnerabilities that customers provides to the criminals. Fraudsters are more systematized and use increasingly sophisticated methods to obtain and misuse consumer personal and financial information (Sakharova & Kha, 2011). Hence, it is not surprising that the rate of contactless card fraud overtook cheque fraud in the first half of 2017, hitting £5.6million. (Sara, 2018).

Due to ignorance, the opportunity to carry out this fraud increases. This study refers to the components of the Fraud Triangle and Fraud Diamond to assess this phenomenon. Having the similar elements of pressure or motive, opportunity and rationalisation with the only difference being the element of capability in the Fraud Diamond (Hermanson, 2004), this study focuses on "opportunity" as it aims to test the loopholes in the security mechanism which can act as the main opportunity for fraudster to seize and to commit contactless cards frauds. This theory has also been used by Subramayen (2008) and Kranacheret (2011) to proof that opportunity is given by the issuers and end users to fraudsters such as in the case of electronic pickpocketing whereby the fraudster is able to gain access to the card due to the inattention of the end users' or the issuers' poor controls on AI and cryptography.

The sufficiency of the contactless card security features in line with the perception of the types of fraud and risk would be an important factor for financial institutions to consider before enhancing the perceived risk of contactless cards. This study will be focusing mainly on the most popular type of frauds namely, relay attacks, electronic pickpocketing, cloning through illegal devices on dark web and theft of cards. Nevertheless, there are various types of security features such as two factor authentication process, cryptography, RFID wallets and the use of AI which have been adopted to prevent contactless cards frauds from prevailing. However, the main question here is whether these types of security features are sufficient enough to prevent frauds. Similarly, this study will refer to the General Deterrence Theory (GDT) to understand what could deter the fraudster. The theory suggests that the fear that the fraudster will get future punishment discourages or deters transgressing of social norms expressed through

DOI: 10.37200/IJPR/V24I2/PR200413
Received: 19 Dec 2019 | Revised: 04 Jan 2020 | Accepted: 15 Jan 2020

the law (Francis T.Cullen, 2009). This study focuses on the prevention mechanism whereby it will test the sufficiency of the security mechanisms imposed on contactless cards such as the two-way authentication process, AI or cryptographic codes in preventing the major types of frauds associated. This will in turn help to raise awareness and inhibit fraud which could prevent crimes including contactless cards frauds before they are carried out (Yan Chen, 2015).

The implementation of new security mechanisms will increase the cost to issuers of contactless cards and may not be necessary since the existing security is sufficient (Swartz, 2006). Cryptography, RFID wallets and the two-factor authentication is a good stopgap to help consumers protect themselves from contactless cards frauds (Kelly, 2015). Contactless cards contain a small and smart microprocessor chip based on public-key cryptography which helps to secure user's credentials. Each card contains a unique public and private key pair that is used during authentication. When prompted by the terminal, the card uses one key to generate a valid cryptographic code that is sent back to the terminal. This code is unique to that transaction and proves that the card is genuine(Gemelto, 2018). Additionally, RFID wallets is a type of wallet which uses a solid layer of material that acts as an armour for the contactless card. This prevents RFID technology signals from reaching inside the wallets which makes this security feature sufficient to prevent relay attack.

In various end user perspective studies from Switzerland (Killer et al, 2015), Australia (Nigel, 2016) and India (Pillai & S.Sathyalakshmi, 2014) it was found that contactless cards with the RFID technology are more prone to relay attacks, electronic pickpocketing, thefts of card and cloning. A relay attack consists of an attacker forwarding a communication between two legitimate endpoints, without the users' knowledge. The fraudster would need to be within a range of 1-10 cm to be able to hijack the communication between the reader and card to sniff the traffic. A relay attack has serious security implications since the attacker can bypass any application layer security protocol, even if such protocols are based on strong cryptographic principles(Francis, et al., 2005)**.**Electronic or digital pickpocketing is the process of stealing data or cash from contactless card in public places (crowded places) using RFID wireless technologies via a cheap gadget that can requires the same frequency and slight connection with the wallet to transfer the account details to the device. Even though some of the data could be encrypted with the CVV code, the fraudster will be able to collect the card number and the expiry date which sufficient information to clone the card(Macbean, 2014).A study in Poland and UK found that smart contactless cards are vulnerable to cloning using devices readily available on the Dark Web (Courtois et al, 2013). It was claimed that a group of criminals called CC Buddies were selling a new hi-tech device on the Dark Web which allowed fraudsters to copy customers' information from their contactless debit cards if the victim is as close as 8 centimetres. The device is called Contactless Infusion X5 and it can copy up to 15 contactless cards per seconds including details such as the card holder's name, card number, expiration date, home address, mini statement which is available in the RFID chip. Costing a mere 1.2 Bitcoin in 2016, the creators of the device further attracted fraudsters by bundling the X5 device together with a USB cable for charging and data transfers, and 20 blank plastic cards so that the fraudster can easily counterfeit the cards(Cimpanu, 2016).

DOI: 10.37200/IJPR/V24I2/PR200413
Received: 19 Dec 2019 | Revised: 04 Jan 2020 | Accepted: 15 Jan 2020

The above authors found that the existing security mechanisms such as AI, cryptography and the two-way authentication process insufficient and recommended stronger security features to prevent fraud in the future.A two-factor authentication process is a security mechanism that requires two types of credentials for authentication and is designed by banking institutions to reduce a breach in security. The authentication can be in different forms namely biometric forms whereby the latter will have to prove their identity through PIN, fingerprints or other devices (Quibria, 2008).

The focus was to decrease the factors affecting the perceived risk perception on contactless cards. These factors were ease of usability, usage behaviour, frauds and security features associated. The high level of usage behaviour and frauds of cards in Australia contributed to the increased level of perceived risk associated with contactless cards, with the high literacy rate in Australia possibly boosting the adoption of the technology compared to developing countries (Nigel, 2016). In Slovakia, findings indicated that security features, usage and frauds has a significant impact on the level of perceived risk associated with contactless cards with the security mechanisms imposed by the bank being deemed sufficient to deter the risk and frauds such as cloning and theft of cards (Vejačka, 2015). Pillai &S.Sathyalakshmi (2014) recommended that the providers of contactless cards in India need to upgrade the authentication system from two to three processes to easily detect any unusual activity on any card.

A study in the USA contradicted the above findings as it highlighted the higher level of security of the contactless smart cards as compared to the normal debit or credit card, hence predicting that the probability of any fraudulent activity to be low (Quibria, 2008). The author believed that the two-way authentication code for the encryption made it impossible to hack into a stolen card since it changed every few seconds. In addition, even though the PIN is not required as a standard payment procedure, the POS terminal will randomly ask the user to enter its PIN (Symon, 2018) providing an additional security to detect if the card has been stolen or cloned. In addition, contactless cards deal with low value transactions, hence the financial loss faced by the customers would be minimal if not zero due to the banks zero-liability policy. The zero-liability policy is for cardholders from the banks that will provide assurance in the event of any fraud.

Studies based on the issuers and banks perspective also reported inconclusive results. RFID-enabled cards are prone to relay attacks, terrorism frauds and distance fraud attacks(Jannati, 2015).Using computer science software and flowchart programming, the author argued that the RFID technology is a threat to authentication protocols used in the systems. RFID security features such as the two-factor authentication is considered as the maximum level of security that can be imposed on contactless cards to reduce the frauds associated with it (Jannati, 2015).

Boden (2016) concluded that contactless cards are troublesome and that the issuers of contactless cards mainly Visa Paywave and Mastercard Paypass had not done their best to ensure the security and safety of the transaction. It is believed the biometric forms of authentication offer significant opportunities to achieve the right balance between convenience and security, however, it is also recommended that customers take responsibility of the cards as well regardless of the zero liability policy.

DOI: 10.37200/IJPR/V24I2/PR200413
Received: 19 Dec 2019 | Revised: 04 Jan 2020 | Accepted: 15 Jan 2020

A study in Ireland found that the security in place such as limits on the value of transactions and random PIN checks was enough to alleviate the fears of end users and to prevent frauds such as relay attacks and electronic pickpocketing (Duke, 2012). In Nigeria, the contactless cards security aspects were deemed to be sufficient, reduced the risk of being robbed since it reduced the carrying of fiat money, in turn reducing the rate of social crime in Nigeria and could also be used as a tool to fight corruption and money laundering (Olusola, et al., 2013). A UK based study claimed that contactless cards such as Mastercard Paypass and Visa Paywave had robust fraud detection and prevention techniques using AI to secure the payment transactions (Erenhouse, 2018).

AI helps to reduce contactless cards frauds as it leverages account information such as customer value segmentation, risk profiling, location, merchant, device data, time of day, and type of purchase made(Nandikotkur, 2018). AI uses analytics and advanced fraud monitoring systems along with dynamic tokens and scorecards to secure contactless cards transactions. Recently, MasterCard has introduced Decision Intelligence as a comprehensive decisioning and fraud detection service to detect normal and abnormal usage behaviour of customers. Based on the interviews with top management of the issuers of contactless cards, the author concluded that the security mechanisms implemented were strong and robust that it is practically impossible for a fraudster to bypass. The finding also highlighted that electronic pickpocketing, relay attacks and even fake POS are just myths since getting access to a certified POS terminal is quite difficult for fraudsters.

III. RESEARCH METHODOLOGY

This study would be using the sequential explanatory mixed method. Questionnaires were distributed to end users to assess the perspective of individuals on the level of risks on contactless cards and the sufficiency of the contactless cardssecurity measures. Based on the feedback obtained, key results were shared with representatives from four banks in Malaysia and interviews were carried out to know their perspective on the sufficiency of security features for contactless cards in comparison to the end user perspective.

DOI: 10.37200/IJPR/V24I2/PR200413
Received: 19 Dec 2019 | Revised: 04 Jan 2020 | Accepted: 15 Jan 2020

Conceptual Framework

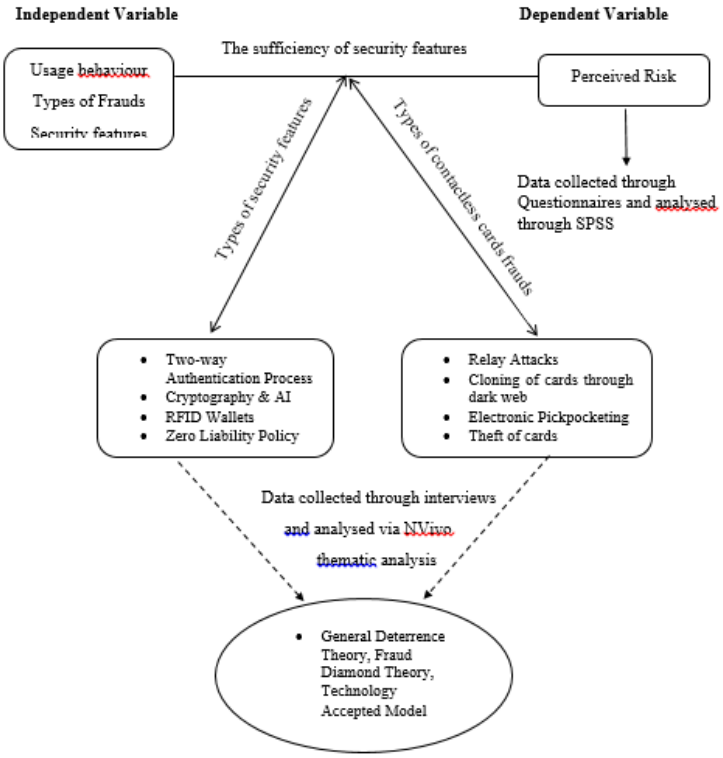


Figure 3.1: Conceptual Framework

Source: Self Authored

IV. DATA ANALYSIS AND DISCUSSION

From the 192 questionnaires collected in Kuala Lumpur from the ***end-user's perspective*** from different age group and income level, it was revealed that degree holders are most likely to use their cards monthly while those who possess a Master prefer to use them weekly. Income level ranging from RM 6001-RM 8001 has the high level of usage for weekly as well as those between the age of 26-30 years old. However almost 80% of them admitted of being unaware of the types of risks and security features of contactless cards.

Table 4. 1: Pearson Correlation

		Perceived Risk	**Usage**	**Fraud**	**Security**
Perceived Risk	Pearson Correlation	1			
	Sig. (2-tailed)				
Usage	Pearson Correlation	.628**	1		
	Sig. (2-tailed)	.000			
Fraud	Pearson Correlation	.329**	.509**	1	

DOI: 10.37200/IJPR/V24I2/PR200413
Received: 19 Dec 2019 | Revised: 04 Jan 2020 | Accepted: 15 Jan 2020

	Sig. (2-tailed)	.000	.000		
Security	Pearson Correlation	-.521**	.388**	.638**	1
	Sig. (2-tailed)	.000	.000	.000	
**. Correlation is significant at the 0.01 level (2-tailed).					

Pearson Correlation test was carried out to find the strength of the relationship between perceived risk and the independent variables. The results were generated through the use of IBM SPSS software 25 and the results are shown in Table 4.19. There is a positive and strong correlation between perceived risk and usage behaviour of customers with r being 0.628. It means that if more customers decided to increase their use of contactless cards, this will increase the perceived risk associated with the cards. This relationship was statistically significant at 1% (0.01) significance level since p = 0.000. Secondly, the correlation between perceived risk and fraud was 0.329 which indicated a moderate positive relationship. In other words, it highlights that in case the level of fraudulent activities rises, this will tend to increase the perceived risk associated with contactless cards and vice versa. This correlation was significant at 1% (0.01) level since p=0.000. The results show a moderate negative correlation between perceived risk and the security features (r = -0.521). This implies that if the level of security features decreases, this will increase the level of perceived risk associated with contactless cards. This correlation was statistically significant at 1% level (p=0.000).

Regression Model

Regression is another statistical tool that can be used to analyse the relationship between two variables. A multiple regression analysis was run using IBM SPSS 25 to assess whether there is statistically significant relationship between the set of variables. In this regression analysis, the researcher took perceived risk as its dependent variable, classified usage behaviour, frauds and security as independent variables to complete the regression model. The multiple regression analysis includes the Model Summary table which measures R-square, ANOVA table presenting F-stat value and coefficient table to test the regression equation.

The results are tabulated as follows:

Goodness of Fit Model

Table 4. 2: Model Summary

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin Watson Stat
1	.725[a]	.680	.602	.36063	1.793

a. Predictors: (Constant), Security, Usage, Fraud

DOI: 10.37200/IJPR/V24I2/PR200413
Received: 19 Dec 2019 | Revised: 04 Jan 2020 | Accepted: 15 Jan 2020

The first table in the Multiple Regression Analysis is the Model Summary which provides goodness of fit measures between the variables. The overall correlation coefficient (R) between the dependent variable and the independent variable was 0.725. This showed that there is a strong positive correlation between the usage behavior, frauds and security. The next important element in the table is the coefficient of determination which is the **(**R^2) value of 0.680. The R square showed that 68% of the variability in the perceived risk of contactless cards could be explained by the independent variables and the remaining 32% can be explained by other factors which had not been included in the model. The value of R square is also considered as a way to check whether the model in reliable. Normally, a minimum R square of 0.6 is considered as reliable. In this study, the R square is more than 0.6 which makes the regression model effective. Finally, the Adjusted (R^2)was 0.602 and it is only a modified version of R-squared that has been adjusted for the number of predictors in the model. As such, it showed that almost 60.2% of perceived risk could be explained by the independent variables.

Coefficient of Analysis

Table 4. 21: Coefficient of Analysis

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.306	.402		5.743	.000
	Usage(U)	.576	.121	.175	2.276	.024
	Fraud(F)	.285	.119	.221	2.399	.017
	Security(S)	-.477	.077	-.408	-3.579	.000
a. Dependent Variable: Perceived Risk						

The coefficient table helps in building the regression line. Beta is the regression coefficient and it is the slope/gradient of the regression line. From the above table, the coefficient (beta) for usage, fraud and security are 0.576,0.285 and -0.477 respectively. As such, the regression equation in this research will be :

Y = 2.306 + 0.576U + 0.285 F -0.477 S

Based on the equation, it can be said that the coefficient β_1 illustrates that if usage behaviour of customers increases by 1%, the perceived risk associated with the cards will increase by 0.576% assuming that all the other variables remain constant. It is also to be noted that there is a positive relationship between the usage behaviour of customers and perceived risk associated with contactless cards. This relationship is significant at 5% level. The second coefficient illustrates that if the level of fraudulent activities such as relay attacks, electronic pickpocketing and thefts of cards increase by 1%, the perceived risk will increase by 0.285% with all other variables remaining unchanged. With a p value of 0.017 this indicates that fraud is statistically significant at 5% level. The last coefficient shows that if the security features of contactless cards increases by 1%, this will decrease the perceived

DOI: 10.37200/IJPR/V24I2/PR200413
Received: 19 Dec 2019 | Revised: 04 Jan 2020 | Accepted: 15 Jan 2020

risk associated with contactless cards by 0.477%. Regardless of their negative relationship that exist between perceived risk and security features, they were statistically significant at 5% level.

Table4.22: Comparison between end users and banks

Types of frauds & Security Mechanisms	**Users' Perspective**	**Banks' Perspective**
Relay attack & Two-way authentication process	More than 77% of the respondents agreed that this security mechanism is sufficient to prevent relay attack.	Relay attack is one of the most prominent frauds of contactless cards, but the two-way authentication process is not sufficient to prevent relay attacks in Malaysia.
Electronic Pickpocketing and RFID Wallet	80% of the users feel safer when they possess a RFID wallet.	Electronic pickpocketing is quite difficult for fraudster to perform transaction and RFID wallets are not necessary to prevent electronic pickpocketing.
Cloning via dark Web, cryptography and AI	79% respondents believe that the use of cryptographic codes is sufficient to prevent cloning. 85% agreed that AI would help in detecting and finding unusual trends of transactions	Cloning cannot be classified as a major type of contactless card fraud because it is impossible to hack or counterfeit the CVV code present behind the card. As such cryptography and AI are sufficient to prevent cloning.
Theft of cards and Zero Liability policy	84% of the end users highlighted that the zero-liability policy are more than enough to prevent them from losses.	Theft of cards can happen due to the carelessness of end-users but with the zero-liability policy, bank ensure that their money is safe making the security mechanisms sufficient

Source: Primary data

The results of regression reflect that all the independent variables including usage behaviour, types of fraud and security features were significantly related to the perception of risk due to the p value less than 5%. The Pearson Correlation revealed that the types of frauds and usage behaviour has a positive relationship with perceived risk as compared to security features which had a negative relationship with perceived risk of contactless cards frauds. The most significant factor affecting the perception of customers was security features whereby when there is an increase in the level of security features, end-user's perception on perceived risks decrease by 0.477 which in turn will motivate them to use more contactless cards for their purchases.

DOI: 10.37200/IJPR/V24I2/PR200413
Received: 19 Dec 2019 | Revised: 04 Jan 2020 | Accepted: 15 Jan 2020

Relay Attacks and Two-way Authentication Process

The interviewees from the banks did not acknowledge any known relay attacks, however confirmed that the two-way authentication process was an effective tool to mitigate relay attacks. The respondent working with Bank Negara Malaysia also emphasised that the contactless cards had undergone stress test prior to being released. The respondents also agreed on the evolvement of the two-way authentication process but in different ways, with Respondent 2 highlighting the future three-way authentication process in 2020 which is more capable to detect relay attacks in Malaysia, Respondent 4 predicting the replacement of the two-way authentication process by biometric authentication etc. implying the insufficiency of the two-way authentication process.

65% of the 192 questionnaire respondents agreed that relay attack is one of the major frauds associated with contactless cards. 57% of them also stated that the two-way authentication process is considered as the main security tool to mitigate relay attacks since it checks the reliability and accuracy of the POS terminal. This clearly indicates that the relay attack is one of the most prominent frauds of contactless cards and that the two-way authentication process is insufficient to prevent relay attacks. However, the banks are upgrading this security feature.

Although the study by Kelly (2015) and Quibria (2008) highlight the two-way authentication as sufficient to prevent relay attacks, the results of this study is consistent to Cristofaro et al (2014) and Narasimham&Padmanaban (2013) in recommending further security measures such as random PIN checks to mitigate relay attacks.

Cloning via dark web, Cryptography and Artificial Intelligence

All four interview respondents agreed that contactless cards cannot be cloned. Respondent 1 believes that cloning was only possible with old chips. The new cards has been encrypted with security features such as random algorithm (Respondent 1), cryptographic code (Respondent 2 and 3) and the inability of the fraudster to obtain the CVV code (Respondent 4) and hence could not be cloned. However, 74% of the end-users believe that the card could be cloned easily through Dark Web but 79% find that cryptographic codes are sufficient to prevent cloning.

Most of the respondents agreed that AI and Machine Learning has been used for quite a long time by banks to prevent frauds such as cloning. Respondent 3 claimed that AI uses predictive analytics to go through billions of transactions to check for any unusual transaction. 85% of the customers agreed that AI is sufficient to detect and prevent cloning. It can be summarised that cloning is not a major issue for contactless cards since the cryptographic codes and AI are sufficient to prevent the fraudster from obtaining the CVV code behind any contactless cards.

The use of cryptographic codes and AI have made it impossible for fraudsters to clone and use the card (Nandikotkur, 2018; Roland & Langer, 2013). Courtois et al (2013) contradicts this by highlighting that contactless cards are quite prone to cloning due to a device called Contactless Infusion X5 which is readily available on the Dark Web. The same study carried out in Poland and UK also found that cryptography and AI are insufficient to prevent cloning. The security features associated with contactless cards to prevent cloning are insufficient (Cimpanu, 2016).

DOI: 10.37200/IJPR/V24I2/PR200413
Received: 19 Dec 2019 | Revised: 04 Jan 2020 | Accepted: 15 Jan 2020

Electronic Pickpocketing and RFID Wallet

The interview respondents questioned the authenticity of the online video on electronic pickpocketing claiming that the fraudsters would only be able to access the card number and expiry date which would be insufficient to perform any transaction. Respondent 2 and 3 did not deem it necessary for users to buy an RFID wallet as having more than one contactless card would create a disturbance for the fraudster's device. Caney et al, (2013) and Gutman (2014) agree that the RFID wallet is irrelevant and was created as just another money making gimmick since the loopholes lie in the fabrication of cards. As long as users have more than one card in their wallet they are safe.

In contrast, 81% of the users believed that electronic pickpocketing is the easiest way for fraudster to get access to their information and almost 80% of the users claimed that they will be safer if they had the RFID wallet since they believe that it might block electronic pickpocketing attempts. Kelly (2015) advocated the need for a RFID wallet as it prevents electronic pick pocketing cases by blocking RFID waves.

Theft of cards and zero liability policy

The banks representatives were asked to comment on the procedures involved for the loss of cards and the sufficiency of the zero-liability policy in protecting the end-users. Respondent 1 and 2 agree that users should inform their respective banks within 24 hours of losing their cards and that the bank will respond with a series of personal questions to confirm the identity of the users and upon receiving the biometric verification, a new card will be issued. Respondent 2 found that the fraud monitoring system is robust and users are normally alerted on any unusual activities on their cards. Respondent 1 further clarifies that banks do not solely take responsibility for the loss of the card and it should be the responsibility of the customer to ensure the safekeeping of the card. Respondent 3 highlighted the sufficiency of zero liability policy set by banks to protect the victims from any liabilities. This is consistent with 89% of the end user's perception, where the first step of action would be to inform the respective banks to block their lost RFID cards, having trust in the sufficiency of the bank's zero liability policy to prevent losses. Studies by Boden (2016), Smith (2017) and Sullivan (2010) conclude the same; highlighting that banks should be the first point of contact in terms of the loss of cards, whilst cautioning that although the zero liability policy provides assurance to the end user, it is also the responsibility of the user to keep the card secure.

Both groups concur that relay attacks is the most prominent fraud affecting contactless cards. However, they differ in terms of the electronic pickpocketing video and the cloning of cards which banks believe is impossible due to the presence of the CVV code behind the cards. Surprisingly, the users believe in the sufficiency of the two-way authentication process in preventing the relay attack, which is disputed by the banks. This could be due to the lack of knowledge by the end users on how the two-way authentication process works. Similarly, users feel safer with a RFID wallet since they believe it protects the electronic waves from reaching their cards and that the risk of cloning through the Dark Web can be reduced by using AI and cryptography. Most respondents also trust the financial institutions zero liability policy to protect them from fraud related losses, including the traditional theft of cards. However, banks and financial institutions are cautious to also hold the users accountable for the safekeeping of their cards.

DOI: 10.37200/IJPR/V24I2/PR200413
Received: 19 Dec 2019 | Revised: 04 Jan 2020 | Accepted: 15 Jan 2020

V. CONCLUSION

The respondents from the banks reflected that sufficient education measures for end-users have taken place, and that the end-users are aware of the risks and security features of the contactless cards. For example, end-users believed that the two-way authentication process isinsufficient to prevent relay attacks, instead it should be reinforced to three-way authentication process to prevent any relay situation. Cloning is another type of frauds associated with contactless cards which can easily be done through devices available on the Dark Web.

Banks promptly denied that such scams are impossible, claiming that AI and cryptography are sufficient to prevent this type of scam. Furthermore, electronic pickpocketing has been claimed to be impossible to occur due to the EMV chip and that user's do not really require RFID wallets for protection as long as there is more than one card in their wallet. Lastly, the banks concluded that theft of cards are not the sole responsibility of the banks but also the users. Therefore, it can be summarised that the end-users believe that the security features of the contactless cards are insufficient with the banks contradicting this.

Recommendationand Conclusion

The findings of this study provide several important practical implications for the promotion of contactless cards since most of the users of contactless cards are not aware of the risks faced andbelieve that the security features are weak. The perceived risk factors directly influence the consumer preference to pay by contactless card their monitoring and investigations, whilst handing more severe punishments to perpetrators of these crimes including hackers. The use of Artificial Intelligence, Machine Learning, Deep Learning etc. could also assist to detect fraudulent transactions to reduce cloning, electronic pickpocketing and identity theft both in the Dark Web and traditional banking process.

REFERENCES

1. Abdullahi, M., 2015. Concomitant Debacle of Fraud Incidences in the Nigeria Public Sector : Understanding the power of fraud triangle theory. *International journal of academic research* , 5(5).
2. Abd, Z. E. & Abokabera, E., 2015. Evolution in bank cards security, cardholder verification and its impact on fraud crimes. *The International Arab Forensic Science and Forensic Medicine Conference* .
3. Boden, R., 2016. *NFO World Plus.* [Online] Available at:https://www.nfcworld.com/2016/07/14/346178/europeans-keen-use-biometric-authentication-payments-says-visa/
4. Campbell, K., 2018. Police warn WA businesses to reduce 'tap-and-go' technology. *The West Australian.*
5. Caney, R. et al., 2013. Mobile Pickpocketing: Exfiltration of Sensitive Data through NFC-enabled Mobile Devices. *Carnegie Mellon University.*
6. Chiou & Shen, 2012. The antecedents of online financial service adoption: the impact of physical banking services on internet banking acceptance. *Behaviour and Information Technology,* 31(9), pp. 859-871.
7. Cimpanu, C., 2016. *New devices sold on darkweb can clone up to 15 contactless card per second.* [Online] Available at: https://news.softpedia.com/news/new-device-sold-on-the-dark-web-can-clone-up-to-15-contactless-cards-per-second-505200.shtml
8. Courtois, N., Hulme, D. & Grejak, M., 2013. On Bad Randomness and Cloning of Contactless Payment and Building Smart Cards. *Security and Privacy Workshops.*
9. Cristofaro, D., Freudiger, J. & Norcie, G., 2014. Two-Factor or not two factor? A comparative usability study of two factor authentication. *In NDSS Workshop on Usable Security.*

DOI: 10.37200/IJPR/V24I2/PR200413
Received: 19 Dec 2019 | Revised: 04 Jan 2020 | Accepted: 15 Jan 2020

10. Cristofaro, E. D., Du, H., Freudiger, J. & Norcie, G., 2014. A Comparative Usability Study of Two-Factor Authentication. *University of College London.*
11. Daily Mail, 2018. *Daily Mail.* [Online] Available at: https://www.dailymail.co.uk/news/article-5507769/Contactless-boom-fuels-51-surge-tap-fraud.html
12. Deloitte, 2008. *Contactless Payment Technology- Catching the new wave,* United Kingdom: Deloitte Touch Tohmatsu.
13. Dorfleitner, G., 2017. *Fintech in Germany.* Germany: Springer International Publishing.
14. Duke, C., 2012. An examination of the barriers Irish businesses face in the adoption of Near Field Communication technology. *Research Gate.*
15. Eccles, L., 2016. *The Daily Mail.* [Online] Available at: https://www.thisismoney.co.uk/money/news/article-3983972/Police-alert-electronic-pickpocketing-contactless-card-scammers.html
16. Emms, M., Arief, B., Little, N. & Moorsel, A. V., 2013. Risks of Offline Verify Pin on contactless cards. *Financial Cryptography and Data Security.*
17. Erenhouse, R., 2018. Dispelling the Myths: The Reality about Contactless Security. *Mastercard*, 17 January.
18. Eyoboglu, K. & Sevim, U., 2017. Determinants of contactless credit cards acceptance in Turkey. *International Journal of Management Economics and Business*, 13(2), pp. 331-346.
19. Fiedler, M., Keppler, T. & Öztüren, A., 2013. Contactless Payment, a RFID domain and its acceptance by its cardholders. *Cyprus International University, Faculty of Economics and Administrative.*
20. Fiedler, M., Keppler, T. & Öztüren, A., 2014. Contactless Payment, a RFID domain and its acceptance by cardholders. *Cyprus International University, Faculty of Economics and Administrative.*
21. Focus Malaysia, 2018. *Mastercard: Contactless payment continue to grow.* [Online] Available at: http://www.focusmalaysia.my/Snippets/mastercard-contactless-payments-continue-to-grow
22. Francis T.Cullen, 2009. *Taking stock : the status of criminology theory.* UK: s.n.
23. Francis, L., Hancke, G., Mayes, K. & Markantonakis, K., 2005. Practical Relay Attack on Contactless Transactions by using NFC mobile phones. *Information Security Group, Smart Card Centre.*
24. Garg, R. & Jain, S., 2015. Requirement Analysis on Paywave. *International conference on advances in computing and communication engineering.*
25. Gautam, I. & Ignico, M., 2010. The Early Experience with Branchless Banking. *CGAP Focus Note,* Issue 46.
26. Gemelto, 2018. [Online] Available at: The benefits of EMV security with the added convenience of contactless technology
27. Hamspire, C., 2016. A mixed methods empirical exploration of UK consumer perceptions of trust, risk and usefulness of mobile payments. *International Journal of Bank Marketing,* 35(3).
28. Harper, A., 2014. Case study of the impact on businesses and society by mobile contactless card technology. *North central University Graduate Faculty of the School of Business and Technology Management.*
29. Hermanson, W. &., 2004. The Fraud Diamond: Considering the Four Elements of Fraud. *The CPA Journal.*
30. Jannati, H., 2015. Analysis of relay,terrorist fraud and distance frauds attacks. *International journal of critical insfrastructure protection.*
31. Juniper Research, 2017. *Juniper Research.* [Online] Available at: https://www.juniperresearch.com/researchstore/fintech-payments/contactless-payments
32. Karoubi, B., Chenavaz, R. & Paraschiv, C., 2016. Consumer perceived risk and hold of use of payment instruments. *Journal of Applied Economics,* 48(4), pp. 1317-1329.
33. Kelly, K., 2015. *UK Fast.* [Online] Available at: https://www.ukfast.co.uk/blog/2015/07/28/why-two-factor-authentication-is-more-important-than-ever/
34. Killer, C., Tsiaras, C. & Stiller, B., 2015. An Off-the-shelf Relay Attack in a Contactless Payment Solution. *University of Zürich, Communication Systems Group.*
35. Kim, C., Tao, W., Shin, N. & Kim, K.-S., 2010. An Empirical Study of customers perceptions of security and trust in e-payments system. *Electronic Commerce Research and Applications.*
36. Kranacheret, 2011. The Evolution of fraud theory. *American Accounting Association Journal.*
37. Krol, K. et al., 2016. An Exploratory Study of User Perceptions of Payment Methods in the UK and the US. *University Paper College London.*
38. Lee, I. & Souza, S. d., 2018. *The Future of Payments: Contactless Payments.* [Online] Available at: https://www.imoney.my/articles/contactless-cards
39. Liébana-Cabanillas, F., Luna, I. R. d. & Montoro, F., 2017. Intention to use new mobile payment systems: a comparative analysis of SMS and NFC payments. *Economic Research* , 30(1), pp. 892-910.

DOI: 10.37200/IJPR/V24I2/PR200413
Received: 19 Dec 2019 | Revised: 04 Jan 2020 | Accepted: 15 Jan 2020

40. Macbean, N., 2014. *ABC News.* [Online] Available at: https://www.abc.net.au/news/2014-05-30/electronic-pickpocketing-looms-as-next-credit-card-fraud-threat/5486806
41. Mackevicius, J. &. G. L., 2013. Transformational Research of the Fraud Triangle. *EKONOMICA*, 92(4).
42. McMillan, J., 2018. Examining the Perceived Risks of contactless card acceptance in the New Zealand Market. *Department of Management, Marketing and Entrepreneurship.*
43. Nandikotkur, G., 2018. *Bank Info Security.* [Online] Available at: https://www.bankinfosecurity.asia/interviews/securing-contactless-card-payment-transactions-i-4077
44. Narasimhan, H. & Padmanaban, T., 2013. 2CAuth: A New Two Factor Authentication Scheme Using QR-Code. *International journal of Engineering and Technology,* 5(2), pp. 1087-1094.
45. Nigel, P., 2016. *The Truth about contactless payment,* Australia: Central for Internet Safety.
46. Olusola, M., Oludele, A., Chibueze, O. & Samuel, O., 2013. CASHLESS SOCIETY: DRIVE'S AND CHALLENGES IN NIGERIA. *International Journal of Information Sciences and Techniques.*
47. Paul, C. L. et al., 2011. A field study of user behavior and perceptions in smartcard authentication. *HCI.*
48. Pillai, D. S. & S.Sathyalakshmi, 2014. Prevention of Relay Attack Using NFC. *International Journal of Innovative Research in Computer and Communication Engineering.*
49. Pratt, B. D., 2006. The empirical status of deterence theory: A meta analysis.
50. Quibria, N., 2008. The Contactless Wave: A Case Study in Transit Payments. *Federal Reserve Bank of Boston.*
51. Raza, S., 2016. The Henry Fund Investment Thesis On Visa Inc.. *VW.*
52. Rogers, 2003. *Diffusion of Innovation.* 5th ed. New York: Free Press.
53. Roland, M. & Langer, J., 2013. Cloning credit cards: a combined pre-play and downgrade attack on EMV contactless. *Proceeding of the 7th Usenix Conference on Offensive Technologies.*
54. Sakharova, I. & Kha, L., 2011. Payment Card Fraud: Challenges and Solutions. *The University of Texas at Dallas,* Volume 5.
55. Sara, S., 2018. Contactless card fraud overtakes cheque scams for first time. *The Telegraph.*
56. Shin & Lee, 2014. The effects of technology readiness and technology acceptance on NFC mobile payment services in Korea.. *The Journal of Applied Business Research,* 30(6), pp. 1615-1626.
57. Simpson, J., 2016. *The Times.* [Online] Available at: https://www.thetimes.co.uk/article/gangs-use-the-dark-web-to-trade-contactless-card-data-dzqppsx6k
58. Smith, S. L., 2007. Gone in a Blink: The Overlooked Privacy Problems caused by contactless payment systems. *Smith Articile,* 11(1).
59. Storm, D., 2013. *ComputerWorld.* [Online] Available at: https://www.computerworld.com/article/2474677/security0/texas-cops-report-victims-of-electronic-pickpocketing-suffer-credit-card-losses.html
[Accessed 5 January 2019].
60. Subramayen, R., 2008. Quality of internal control procedures : Antecedents and Moderating effect on organisational justice and employee fraud. *Managerial Auditing Journal.*
61. Sullivan, R. J., 2010. The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options. *Federal Reserve Bank of Kansas City.*
62. Swartz, D. D. G., 2006. The Move Toward a Cashless Society: Calculating the Costs and Benefits. *Review of Network Economics.*
63. Symon, J., 2018. Detecting relay attacks against Bluetooth communication in Android. *Research Commons at the University of Waikato.*
64. Trutsch, T., 2017. The Impact of Contactless Payment on Cash Usage. *University of St. Gallen.*
65. Vejačka, M., 2015. Consumer Acceptance of Contactless Payments in Slovakia. *Journal of Applied Economic Sciences,* Issue 35, pp. 760-765.
66. Vogues, D., 2017. A study of the NFC market in Germany in cooperation with Fidesmo AB.. *KTH Royal Institute of Technology School of Insustrial Engineering and Management.*
67. Wang, T., 2008. Determinants affecting consumer adoption of contactless credit card: An empirical study. *Cyber Psychology & Behavior,* 11(6), pp. 687-689.
68. Wang, Y.-M. & Lin, W.-C., 2019. Understanding consumer intention to pay by contactess credit cards in Taiwan. *International Journal of Mobile Communications,,* 17(1), pp. 1-23.
69. Weiber & Pohl, 1996. Leapfrogging-Behavior and adoption of the contactless cards. *Journal of business economics,* 66(10), pp. 1203-1222.

DOI: 10.37200/IJPR/V24I2/PR200413
Received: 19 Dec 2019 | Revised: 04 Jan 2020 | Accepted: 15 Jan 2020

70. Widjaja & Ooi, E. P., 2015. Non-Cash Payment Options in Malaysia. *Journal of Southeast Asian Economies.*
71. Yan Chen, K.-W. W., 2015. Organizations' Information Security Policy Compliance : Stick or Carrot Approach. *Journal of Management Information System.*
72. Yilmazer, K., 2006. Adoption of internet banking and consumers payment choices. *Working Paper of Purdue university.*
73. Zaharudin, R. Z. A. R., Rashid, U. K. & Nasuredin, J., 2018. Usage Behavior among Paywave Card Users in Kuala Lumpur. *International Journal of Research.*
74. Zheng, M, F. & Coat, H. P., 2013. Chinese consumer perceived risk and risk relievers in e-shopping for clothing. *Journal of Electronic Commerce Research,* 3(13), pp. 255-274.

DOI: 10.37200/IJPR/V24I2/PR200413
Received: 19 Dec 2019 | Revised: 04 Jan 2020 | Accepted: 15 Jan 2020