“Price Tag” of Risk of Using E-Payment Service

Ho KKW, See-To EWK, Chiu DKW

Abstract

In this research, the authors utilized a survey to evaluate the notional values of the overall risk, the privacy risk, and the financial risk of using a credit card and an RFID-based E-payment service from risk-neutral and risk-averse users. With the known extra financial risk (in terms of monetary value) to be faced by the users in using two different versions of an RFID-based E-payment service, the authors determined the notional monetary value of the extra privacy risk posed by providing personal and financial information to the E-payment service and the differences in the risk aversion of the two groups of users. The findings may help E-payment service developers design better E-payment services based on a better understanding of the value of personal data in their users’ perspectives and, thus, help determine the appropriate incentives for attracting users to use their services.

Keywords: e-payment service; overall risk; perceived risk; privacy risk, risk aversion, RFID

Introduction

E-payment is one of the most popular and vital types of E-services today (Ruiz-Martínez 2015). It is a business with a high-profit margin, as demonstrated by PayPal, which had earnings in 2016 was US$10.8 billion, with a 17% growth compared to 2015 (PayPal 2017). The growth of E-payment services creates a competition between the E-payment service providers and conventional payment service providers, primarily credit card companies and banks. As shown in prior research, most consumers prefer to use a single payment network in their daily lives, even though they may need to use multiple payment networks (Rysman 2007). As a result, banks and credit card companies establish alliances with E-payment service providers to explore collaboration opportunities (PayPal 2016).

E-payment services play a key role in different types of E-services (Kazan and Damsgaard 2016) to assist consumers in transacting online (Ogawara, Chen, and Chong 2002; Tsai et al. 2010; Zhang and Prybutok 2003). While E-payment services may be convenient and easy to use (Lai 2014), prior research shows that consumers are typically not highly motivated to adopt such services, as they perceive E-payment services as risky (Featherman and Wells 2010; Hong and Cha 2013; Martins et al. 2014). To encourage these consumers to use E-payment services, service providers should develop features to prevent Internet fraud and reduce other risks. A stream of information systems (IS) literature focused on investigating ways to reduce the perceived risks of using E-payment services (Siyal et al. 2019; Chang and Wu 2012; Hann et al. 2007; Ho and Ng 1994; Nicolaou and McKnight 2006; Pavlou and Gefen 2004; See-To and Ho 2016; Trivedi 2019). The significant findings of these studies can be summarised as: "The adoption intention of E-payment services will increase if the level of consumers' perceived risk is reduced."

While most prior studies focused on developing methods and procedures to reduce consumers' perceived risk level, Hann et al. (2007) explored the possibility of trading off the privacy risk of online consumers through the provision of benefits such as monetary rewards and usage convenience to consumers based on a research model developed from information-processing theories. Through collecting data from an experiment, the researchers used conjoint analysis to analyse responses from Singapore and the United States and to estimate the value of privacy protection of websites, which was between US$30.49 and US$44.62. As inspired by Hann et al. (2007), the study authors wanted to evaluate the monetary value of the privacy risk of using E-payment services and use the information as a proxy to discover the notional monetary value for the difference between risk-neutral and risk-averse users. The result of this study can help online service providers gain a better understanding of the notional value of privacy risk by comparing this study's results with that of Hann et al. (2007). As such difference represents risk aversion (Chiu et al. 2009), the authors' findings may offset the negative impact of these risk factors and encourage online users to utilize the more profitable and convenient, but riskier, E-payment services through the provision of monetary rewards. As a result, this study's findings can enhance the adoption intention of various types of E-services that involve payments as one of their key components.

Thus, the findings of this research have both theoretical contributions and managerial implications. First, the authors developed a method based on risk theory to determine the monetary value of the privacy risk and the difference of risk averseness of two different types of online consumers. Plus, the result of this study can help E-payment service providers develop new mechanisms, which motivate users to use monetary rewards to offset the perceived risks of using their services. This is particularly, important, as prior research shows the importance of considering customers' opinions in developing new service innovation projects (Abramovici and Bancel-Charensol 2004) among which E-payment services are key representatives.

This study is presented as follows: After the Introduction, the authors present a review of the literature on E-payment services and the perceived risks. Then, the authors introduce their research methodology, followed by information about the data collection and data analysis. At the end of the paper, the authors discuss the theoretical contributions, practical implications, and the limitations of this study, as well as the future research directions.

Literature Review

Prior researchers in finance and economics have studied the use of E-payment services for decades; in particular, the use of credit cards and debit cards in the online environment . One of the reasons that researchers are interested in the credit and debit card industry is due to its characteristics of networked services, which link up both consumers, financial institutions, and sellers (Chakravorti 2003). In particular, researchers want to understand when and why consumers use a credit card or debit card for electronic payments for a specific scenario. For example, Carow and Staten (1999) conducted a survey using gasoline consumer participants to study this issue. They noted that credit card users are more educated and have more income compared with users who use cash to transact their payments, and anticipated that debit card users had similar characteristics to those of credit card users. Zinman (2009) further studied this issue by using panel data obtained from the USA, and discovered that consumers facing higher credit card (financial) charges were more likely to use a debit card to avoid the financial charges. This suggests the need for a slight change in the design of a payment service that would influence the consumer's choice of using or not using that payment service.

Another major factor affecting the selection of using an E-payment service is the risk associated with using that service. Prior research on perceived risk can be found in literature about information systems (IS) researches and marketing. One commonly used definition of perceived risk was defined by Bauer (1960), as "risk will produce consequences which (consumers) cannot anticipate with any approximate certainty and some of which, at least, are likely to be unpleasant." Prior IS research has employed at least two methods to probe into the perceived risk issue. For example, Kim et al. (2008) and Ho and Awan (2019) measured the perceived risk on E-payment services as a single construct in their research model to see how the perceived risk would affect the adoption and use of E-payment services, and E-commerce in general. On the other hand, other IS researchers, such as Ho and Ng (1994), Featherman and Wells (2010), Martins et al. (2014), See-To and Ho (2016), Stone and Grønhaug (1993), and Yang et al. (2015) analysed perceived risk as a multidimensional construct. They investigated the impact of perceived risk based on different aspects, including financial risk, privacy risk, performance risk, psychological risk, social risk, and time risk, as shown in Table 1 (Featherman and Wells 2010). Prior research has shown that financial and privacy risks are the two most influential aspects of risk in using E-payment services (See-To and Ho 2016; Yang et al. 2015), compared with the other four aspects. Prior research also reported that these two aspects of risk could be mitigated by manipulating the design of E-payment service systems (See-To and Ho 2016). Therefore, in this study, the authors focused on reviewing these two aspects of risk.

[Place Table 1 near here]

Among the different types of perceived risk that may impact the adoption of E-commerce and E-payment services, financial risk has been extensively studied. Financial risk has been considered the most important factor in perceived risk as indicated in the literature for decades (Peter and Ryan 1976). In the E-payment service context, Bhatnagar et al. (2000) studied the impact on E-commerce and showed that financial risk is one of the key averse factors on the adoption of using online payments for E-commerce services. Hong and Cha (2013) further distinguished financial risk and online payment risk, and showed that both risks adversely affect online payment intentions. However, these risks did not appear to affect perceived trust in payment services.

There are extensive research studies on finding ways to reduce financial risk. Ho and Ng (1994) reported that money-back guarantees provided by E-payment services could help reduce the financial risk faced by consumers. See-To and Ho (2016) investigated the E-payment service design issue and suggested that monetary rewards and reducing consumers' liability for losses (as an alternative version of the money-back guarantee) could both reduce the financial risk and encourage users to consider using E-payment services. Lee et al. (2012) also studied the relationship between the level of financial risk faced by users and the level of security provided by E-commerce payments. They noted that there is a trade-off between financial risk and security convenience.

Another important type of risk affecting the adoption of E-payment services is the privacy risk. Privacy risk has been known to be an obstacle for some people with regard to adopting E-services (Liu et al. 2011). As most E-payment services in the market today use online transaction methods, many users worry about Internet security and, in particular, the possibility of leakage of personal information during transactions (Hong and Thong 2013; Liao et al. 2011). However, many users are not familiar, and are not aware of, how much privacy risk they are facing when using these services (Robinson 2017). Bergström (2015) showed that online users were more concerned about privacy risk when they were using E-payment services, compared with other services online, such as email or online searches. Consumers are willing to pay more for subscribing to E-payment services with a higher level of security to reduce their privacy risk (Tsai et al. 2011). A study by Kim et al. (2010) showed that perceived security could encourage users to use E-payment services. Additionally, research by Hirschprung et al. (2015) developed a methodology to estimate privacy risk in E-payment environments. Further, See-To and Ho (2016) reported that the negative impact of privacy risk for an E-payment service could be reduced through incorporating suitable E-payment service design mechanisms, such as an anonymous payment method.

Recently, more researches focus on the privacy risk on mobile payment services, i.e., those specifically used for mobile commerce, which has become a trendy version of E-payment services. Research findings suggest that privacy risk can influence the users' perceived security on the system and reduce the users' trust in mobile commerce (Al-Khalaf and Choe 2020). Yet, the cultural background of mobile payment service users can influence their responses towards privacy risk (Chen, Zhang, and Lee 2013).

The literature also studied why users have a different level of attitude towards risks. From the angle of behavioural economics, Kahneman and Tversky (1979) suggested that the risk-averse nature of humans would affect their decision-making. They suggest that people are either risk-neutral, meaning they would not avoid risk (referred in this study as an H-type risk-taker), or risk-averse, meaning they would avoid risk in their decision-making processes (referred to as an L-type risk-taker).

This research study investigates how the risk attitude of users (H-type vs. L-type) relates to their choice of using a different version (low risk vs. high risk) of an RFID E-payment service card. Prior research in behavioural economics (Tversky and Kahneman 1981) has also shown that L-type and H-type subjects will make different choices based on their attitudes towards risk. Liu and Forsythe (2010) added that H-types would act as "benefit perceivers" and L-types would act as "risk perceivers." Thus, based on these premises, the authors conjectured that their subjects would choose the type of RFID payment service card based on their risk attitude. Plus, See-To and Ho (2016) suggested that H-type users are more ready to use E-payment services with a risky feature than L-type users, when the risky feature can provide a more convenient service to them.

In summary, the two most significant types of risks faced by E-payment service users are financial risk and privacy risk. In this study, the authors want to discover the notional monetary value of these risks and the difference between the risk aversion levels of H-type and L-type users. With these values known, E-payment service providers can consider developing relevant methods to help alleviate the risk by providing suitable design features or reward schemes to encourage consumers to use their services.

Research Method

Prior research analyses perceived risk in two different contexts, i.e., as a single construct, such as Kim et al. (2008), or broken down into a multidimensional construct, such as See-To and Ho (2016). According to Weber et al. (2002), risk attitude can be expressed as the sum of risks and benefits, where the benefits would reduce the risk attitude. In this study, the authors considered the protection provided by an E-payment service as the major benefit of using the system. Therefore, the perceived risk of using an E-payment system can be expressed by Equation 1:

$$Risk_{Overall,j} = \sum Risk_{i,j} - Protection_j \tag{1}$$

Risk$_{\text{Overall,j}}$ represents the perceived risk in using payment service j, Risk$_{\text{i,j}}$ represents the *i*th aspect of risk by using payment service j, and Protection$_{\text{j}}$ represents the benefits provided by payment service j for reducing the risk.

As mentioned, there are two types of users, i.e., risk-neutral (H-type) and risk-averse (L-type). When the authors include the risk aversion issue to their understanding of perceived risks, they can further expand Equation 1 into Equations 2a and 2b:

$$Risk_{Overall,j,H} = \sum Risk_{i,j,H} - Protection_j \tag{2a}$$

$$Risk_{Overall,j,L} = \sum Risk_{Overall,j,H} - Protection_j + Risk\ Aversion_j \tag{2b}$$

Where the subscripts H and L correspond to H-type and L-type users, respectively.

When the authors developed Equations 2a and 2b, they used the perceived risk of the risk-neutral subjects as the baseline. Thus, the difference between the two kinds of perceived risks (i.e., risk-neutral vs. risk-averse) represents the risk aversion. By measuring the perceived risk of H-type and L-type users on a particular payment service, the notional difference will be the proxy of the "extra" risk aversion of the L-type. If one can have different versions of an E-payment service for collecting the perceived risk level for comparison, and with some of the comparisons linked to monetary values, it becomes feasible to discover the notional monetary value for the risk aversion and some aspects of risk.

In this study, the authors used a Radio-Frequency Identification (RFID) payment card as one of the E-payment gateways for measuring the impact of financial and privacy risks. Prior research has shown that online users using RFID technology have a certain level of privacy concerns (Cazier et al. 2008; Clarke III and Flaherty 2008; Hossain and Dwivedi 2014) and, therefore, the "inborn" nature of the RFID payment card would incur both elements of privacy and financial risks.

The RFID-based E-payment system used in this study is a commonly used payment card in the transportation system of a city in Pacific Asia, which also can be used for micro-payments in supermarkets and convenience stores. As this payment system requires users to deposit money into the card before usage, its operation is similar to a debit card. Currently, there are two types of cards available for this RFID-based E-payment service, i.e., anonymous cards (with a unique card ID), which users are required to deposit cash into the card at train stations and convenience stores, and personalized cards with the user's name imprinted on the card, which gives users an extra option to deposit money to the card through direct debit authorization (with a daily recharge limit of a local currency equivalent to

US$128). As these two types of payment cards do not provide any extra benefits (such as mileage) to their users, they are identical except for the two features mentioned, i.e., the inclusion of the name of the user and the direct debit authorization on the personalized card. Therefore, the personalized card incurs more risk compared to the anonymous card, and therefore poses a higher level of privacy risk. This is because a personalized card has the user's personal information imprinted on the card, and also the bank/credit card account information linked to the account, which for some occasions could be used as the electronic ID for entering into condominium complexes or offices, if those premises have linked their systems to the service provider. As for financial risk, the card can only deposit an amount of local currency equivalent to US$64 into it. An anonymous card user will only lose US$64 at the most, whereas for a personalized card user, the loss of the US$64 stored on the card, plus two recharges of up to US$128, or US$192 assuming the user discovers the loss within a day.

Based on the findings from See-To and Ho (2016), L-type users are more likely to choose the anonymous card, and H-type users are more likely to use the personalized card. In this study, the authors use the choice of an RFID-based E-payment service card as a proxy to separate their users into L-type and H-type. It is because the user needs to go through an application process to obtain the personalized card, which may take about 10 days. Thus, the choice of using a personalized card should not be an impulsive, but a rational, decision. Therefore, the subjects' choices of card type have revealed their risk profile difference, as a risk-neutral subject (H-type) would be more likely choose higher risk products compared to a risk-averse subject (L-type).

As discussed earlier, the authors needed two payment services in order to provide sufficient information to discover the notional monetary values of the risk aversion and some of the dimensions of perceived risk. In this study, the authors use an online credit card payment service and an RFID-based E-payment service as the two candidates for the payment services.

Data Collection and Data Analysis

Data Collection

For this study, data was collected through the use of an online survey to identify the monetary values of privacy risk and the difference in the risk averseness of H-type and L-type users. The online survey website was hosted on the Government-to-Citizen (G2C) E-government portal for four weeks. The portal allowed citizens to create personal accounts and join as "members" of the portal. In this study (which is part of a major study on the E-business survey that contains three different studies), the authors invited the 160,000 registered members of the portal to participate, which was about 2% of the population of the city concerned. The survey respondents were required to have an RFID-based E-payment card from the service selected by the authors, and use the card's serial number to register for the survey. To encourage the citizens to participate in the online survey, the authors provided a small number of cash prizes to the participants through a lucky draw. In total, 1,758 usable responses were obtained, of which 889 respondents (50.6%) were female.

The average age of the subject participants was 30.7 years old. Table 2 summarises the demographic data of the respondents, including their average age, average annual personal income (in US dollars), frequencies of online shopping per year, and educational background.

[Place Table 2 near here]

As reported by See-To and Ho (2016), the choice of an RFID payment card can act as an indicator of the risk attitude (H-type vs. L-type) of the subjects, which the authors also explain is because the choice of the card involved a rational decision. Thus, the RFID card selection result acted as an explicit sign of the risk propensity of the subjects. From Table 2, it can be noted that the H-type users ($\mu = 6.78$) make 1.76 more online purchases than L-type users ($\mu = 5.02$) per year, with $p < 0.001$. This suggests that these two groups of users are different concerning online purchase behaviours. As H-type users are risk-neutral, it is more likely for them to purchase online compared to L-type users. This result echoes the findings of prior research, which indicated that the level of perceived risk had a negative impact on the intention and usage of online shopping (Chang et al. 2005).

Data Analysis

Notional Value of Risk Aversion

In the metropolitan area concerned, the citizens use their credit cards and RFID-based E-payment service cards frequently. It was noted that, on average, each study participant had two credit cards and made 11 transactions with a total of over US$1,500 spent per quarter. For the RFID-based E-payment service card, 99% of the population used the card daily. Therefore, the participants of this study were very familiar with the operations of the two payment methods.

For the design of the data collection process, the Delphi method was used to obtain insights from both E practitioners and users. The Delphi group consisted of 10 practitioners (4 from financial industries, 3 from E-business sectors with involvement in the design of their online retail websites, and 3 from E-service sectors), in addition to 5 student users (2 doctoral students, 2 MBA students, and one undergraduate student with an average of over 10 years of experience making online purchases). The research team designed the survey items as listed in Appendix A, based on the understanding that the subjects to be recruited for participation in the online survey were familiar with the operations and the risks associated with the use of both kinds of cards.

A pre-test of the survey, using undergraduate students, was conducted. A subsequent in-depth interview of the subjects confirmed that the authors' assumptions were correct. The actual survey used a 9-point Likert scale (1 = risk-free; 9 = extremely risky) and the correlation matrix is presented in Appendix B. The authors included an online credit card payment service as the reference point of this study because it is a service that nearly all of the subjects had used before, and it was the most commonly used online payment method. Table 3 summarized the findings.

[Place Table 3 near here]

Using the data presented in Table 3, the authors calculated the difference between the perceived risk and the perceived privacy risk of using the online credit card service by both H-type and L-type users. The difference in the perceived privacy risk of using the online credit card service by H-type ($\mu = 6.7919$) and L-type ($\mu = 6.9266$) users was –0.1347, with $p > 0.1$. This indicated that the H-type and L-type subjects basically viewed the perceived privacy risk of using an online credit card service at the same level, which echoed the assumption of developing Equations 2a and 2b.

The difference in the perceived risk of using online credit card services by H-type ($\mu = 6.3545$) and L-type users ($\mu = 6.6796$) is –0.3251, with $p < 0.001$ indicated that the difference was statistically significant. As shown in Equations 2a and 2b, the difference between perceived overall risk values was the notional value (on the Likert Scale) of the risk aversion for L-type users compared to H-type users. This result indicated that the risk aversion between the H-type and L-type was significant and could be measured in the survey design selected.

Further, it was noted that the perceived risk values for both H-type and L-type users was lower than the corresponding perceived privacy risk values. As indicated in the equation, the lower value of the perceived risk when compared with the privacy risk was due to the protection provided by the payment system, which reduced the perceived risk.

As shown in Table 3, the perceived risk of using online credit card payment services for L-types was higher than H-types, because L-type users are risk-averse. Therefore, when they evaluate the perceived risk of the same service with H-type users, they report a higher perceived risk level. However, for the online RFID-based E-payment service, L-type and H-type users are using a slightly different version of the cards. As mentioned, as the inherent risk nature of the personalized card is higher than the anonymous card, even though H-type users are risk-neutral, they report a high risk for using the cards than L-type users who use a less risky version of the cards.

Notional Value of Privacy and Financial Risk of Using RFID-Based E-Payment Service Card

Table 3 shows that the perceived privacy risk of using anonymous RFID-based E-payment cards for online transactions (that contain no personal information, but only the card ID) by anonymous card users is 5.4689 and the perceived privacy risk of using personalized RFID-based E-payment cards for online transactions (which are linked to the users' credit card accounts) is 5.9152. The difference between these two values, i.e., 0.4463 ($p < 0.001$), is the additional perceived privacy risk of providing the users' credit card account information of using the personalized RFID-based E-payment service card.

To compute the notional value of perceived financial risk, an indirect method was used to examine the perceived risk. From Equation 1, it is known that after subtracting the perceived protections provided by the payment service, the perceived risk is the sum of all aspects of perceived risk. Equation 1 can be further elaborated as Equation 3:

$$Risk_{Overall,j} = Risk_{Financial,j} + Risk_{Privacy,j} + \sum Risk_{i,j} - Protection_j \qquad (3)$$

As detailed in Table 3, there is $\text{Risk}_{\text{Overall,RFIDCard,L}} - \text{Risk}_{\text{Overall,CreditCard,L}} = -1.4318$ ($p < 0.001$) and $\text{Risk}_{\text{Overall,RFIDCard,H}} - \text{Risk}_{\text{Overall,CreditCard,H}} = -0.7726$ ($p < 0.001$). The difference between these two numbers is 0.6592 (i.e., –0.7726 – (–1.4318)). When these two equations are expanded, Equation 4 is obtained.

$$\left(Risk_{Overall,RFID,H} - Risk_{Overall,Credit,H}\right) - \left(Risk_{Overall,RIFD,L} - Risk_{Overall,Credit,L}\right) = \left(Risk_{Overall,RFID,H} - Risk_{Overall,RFID,L}\right) + \left(Risk_{Overall,Credit,L} - Risk_{Overall,Credit,H}\right) \quad (4)$$

From Equations 2a and 2b, it is known that $\left(Risk_{Overall,j,L} - Risk_{Overall,j,H}\right)$ is equal to the risk aversion of L-type users on the respective payment service; and for j = credit card systems, all the terms will be cancelled out and the risk aversion term for the credit card system will remain. Therefore, Equation 4 can be further expanded to Equation 5.

$$\left(Risk_{Overall,RFID,H} - Risk_{Overall,Credit,H}\right) - \left(Risk_{Overall,RFID,L} - Risk_{Overall,Credit,L}\right) = \left(Risk_{Financial,RFID,H} - Risk_{Financial,RFID,L}\right) + \left(Risk_{Privacy,RFID,H} - Risk_{Privacy,RFID,L}\right) + \left(\sum Risk_{i,RFID,H} - \sum Risk_{i,RFID,L}\right) - \left(Protection_{RFID} - Protection_{RFID}\right) + Risk\ Aversion_{RFID} - Risk\ Aversion_{Credit} \quad (5)$$

As shown by researchers See-To and Ho (2016), H-type and L-type users reacted differently when they are dealing with financial and privacy risks, but not to other types of risks. Therefore, it can be assumed that the terms related to the other risks of H-type and L-type users will be cancelled out. Also, by assuming the difference of the risk aversion of H-type and L-type users is constant, risk aversion terms can also be cancelled out. Therefore, Equation 5 can be further simplified to Equation 6.

$$\left(Risk_{Overall,RFID,H} - Risk_{Overall,Credit,H}\right) - \left(Risk_{Overall,RFID,L} - Risk_{Overall,Credit,L}\right) = \left(Risk_{Financial,RFID,H} - Risk_{Financial,RFID,L}\right) + \left(Risk_{Privacy,RFID,H} - Risk_{Privacy,RFID,L}\right)(6)$$

The notional value of the differences between H-type and L-type users for the two kinds of payment services is 0.6592. From previous calculation, it is known that the difference in privacy risk is 0.4463. Therefore, the notional difference in financial risk is 0.2129.

Notional Monetary Values of Risks

While the authors noted that the notional value of financial risk was 0.2129, they also knew the actual difference of the financial risk in monetary terms. For the anonymous RFID-based E-payment service card users, the monetary loss (aka, financial risk) was from US$0 to US$64. This is because, for an anonymous card, a user can only deposit up to US$64 and there is no automatic recharge function. Here, the authors assumed that the prior spending of the card by the user was following a uniform function. The monetary loss (aka financial risk) faced by personalized RFID-based E-payment service card users were from US$0 to US$192. This was because a personalized card has a maximum storage of US$64 and can be recharged once every 24 hours – assuming the user noted the loss by the 24-hour mark, the card would have been recharged up to two times. Therefore, while someone who picks up a lost card of this version may not use it, if that person decides to use it (which is theft), US$192 can be used up (assuming an E-payment service card is fully loaded and can be recharged twice). As this card is the only RFID card used by the transportation system, and can be used in convenience stores and supermarkets, it can reasonably be assumed that the owner would need to use it at least once per day. Therefore, it can further be assumed that the owner would discover the loss of the card within a day and suspended or cancel the card to avoid further financial loss. Based on the assumption that the card user would become aware of the loss of the card within 24 hours, and the card would have been recharged a maximum of two times, the estimated maximum loss would be US$192 (i.e., US$64 × 3). Similar to the model the authors used for the anonymous card, the authors assumed that the initial balance of the card was following a uniform function with a range from US$0 to US$64. That results in the range of the final loss becoming a uniform function with a range from US$0 to US$192.

Therefore, the difference in the maximum financial loss between these two kinds of cards is US$128 (i.e., US$192 – US$64). Assuming that the lost function is a uniform function, the mean lost for anonymous RFID-based E-payment service card users would be US$32, and for the personalized RFID-based E-payment service card users would be US$96. Thus, the difference would be US$64.

As the notional difference (on the Likert Scale) for the loss was 0.2129, therefore, the equivalent monetary value of each unit on the Likert scale ranged from US$300.61 (i.e., calculated based on the average difference of loss of US$64 or US$64 ÷ 0.2129) to US$601.22 (i.e., calculated based on the maximum difference of loss of US$128 or US$128 ÷ 0.2129).

To compare the two kinds of RFID-based E-payment service cards, the users of the personalized card needed to provide their credit card number and their personal information to the company to gain a more convenient service. The authors noted that the notional value of this extra privacy risk is 0.4463 per unit, i.e., from US$134.16 (i.e., US$300.61 × 0.4463) to US$268.32 (i.e., US$601.22 × 0.4463). Applying a similar methodology, the authors noted that the risk aversion was US$97.73 (i.e., US$300.61 × 0.3251) to US$195.46 (i.e., US$601.22 × 0.3251), based on the notional value of 0.3251.

Discussion

Theoretical Contributions and Practical Implications of Notional Monetary Values of Privacy Risk and Risk Aversion

From the authors' calculation, it was noted that the notional monetary value of privacy risk of using personalized RFID-based E-payment service cards, compared with the anonymous RFID-based E-payment service cards, was US$134.16 to US$268.32. This value was treated as the notional value of asking E-payment service users to provide more personal information in using the service.

The value obtained from this study, using Equations 5 and 6, is much higher than that reported by Hann et al. (2007), which suggested the notional monetary value of providing personal information to a website was between US$30.49 to US$44.62. The difference in the notional monetary values found by these two studies arise from the experimental design. Hann et al. (2007) investigated this topic using a laboratory experiment setting with the subjects interacting with a hypothetical website. However, their subjects did not have any real or prior interaction with the website in this controlled (laboratory) setting, and merely guessed about its functionality and the privacy risk of using it.

For this present study, in a sense, the authors extended their enquiry of the privacy risk by conducting an online experiment based on a real product. In this case, the subjects fully understood the functionality and risks of the RFID E-payment service cards, as they used it in their daily lives and did not need to guess its performance. As a result, they included their prior experience (both pros and cons) of using the RFID E-payment service cards in their assessments. While this was an area that could not be fully controlled in this experiment, this study provides a different perspective, as it has significant field elements in this experiment due to the subjects answering the survey based on their real-life interactions with the E-payment service, and not on an imaginary situation. Therefore, the findings reflect a realistic situation and can provide insights for researchers and practitioners into understanding how E-payment service users quantified the privacy risk they faced in using this product.

As for the subjects anticipating a higher notional monetary value for providing their personal information to the RFID-based E-payment card, there may be an explanation. There was a scandal related to the holding company of the E-payment service cards, which sold the personal information that the firm collected through the daily card transactions to six different companies using a loophole of the Personal Data (Privacy) Ordinance in the city concerned. This incident triggered the concerns of the subjects in providing their personal information to the E-payment service card company and resulted in a higher notional monetary value for providing extra personal information.

One of the key practical contributions of this study is the discovery of the notional monetary value of the difference of risk aversion of H-type and L-type consumers by using RFID-based E-payment service cards, which was around US$97.73 to US$195.46. This is the notional monetary value of attracting an L-type user to "upgrade" their subscription from an anonymous RFID-based E-payment service card to a personalized card. Prior research in behavioural economics, such as that of Holt and Laury (2002), has demonstrated that it is possible to measure the trade-off of risk aversion using monetary payoffs. Further, researchers Bergendahl and Lindblom (2007) also showed how the pricing scheme of payment services could stimulate the demand for one type of service over others. Therefore, the notional values found in this study could help practitioners plan for developing new service schemes to encourage users to opt for subscribing service plans with a higher risk level. In particular, E-payment service providers can consider the choice of the services and privacy risk levels (i.e., L-type vs. H-type) to identify the group of L-type users and estimate the notional monetary value risk aversion. Then, they could design a tailor-made marketing campaign to "pay" (i.e., provide financial incentives) L-type users to switch to a service that allows them to legally collect more (private/sensitive) information from their users for planning, promotion, and product design. Actually, in recent years, some E-payment service providers in China, such as Alipay and WeChat Pay, also provide online cash coupons to their users to encourage them to use their services. The rebates are cash discounts provided by the E-payment service providers without notifying the vendors (and thus, the vendors concerned would not know that the customers are using their rebates coupons). This mechanism is similar to what the authors are proposing, however, as far as the authors know, the E-payment service providers currently design the value of the cash coupons based on their experience, rather than using a data-driven approach to estimate the value of the monetary reward to offset risk aversion.

Comparing the financial risk of using the two types of RFID cards, i.e., a maximum potential loss of US$64 and US$192 for anonymous and personalized RFID cards, respectively, with the extra privacy risk of US$134.16 to US$268.32 of using personalized RFID cards, it was noted that the extra privacy risk of using the cards was at least close to, and probably would be higher than, the financial risk of using the cards. This result echoes the findings by See-To and Ho (2016), which stated the negative impact of the utility of E-payment service from privacy risk was –1.889 utility unit for payment with identity and –3.159 utility unit with online data transfer on a 0 to 100 utility-scale, whereas the impact for liability of maximum financial loss of US$128.20 and US$256.40 were –1.362 and –2.242, respectively.

Using the data from See-To and Ho (2016) as a reference, the authors estimated that the unit utility was equivalent to US$94.13 (US$128.20 ÷ 1.362) to US$114.36 (US$256.40 ÷ 2.242). Therefore, the cost for payment with identity was between US$177.81 (US$94.13 × 1.889) and US$216.03 (US$114.36 × 1.889), and the cost for online data transfer for payment was between US$297.36 (US$94.13 × 3.159) and US$682.44 (US$114.36 × 3.159). Thus, it shows that the reduction of the utility of privacy risk can be higher than a known amount of financial risk. The primary reason for this observation most likely comes from the fact that the measure of the financial risk for this study and that of researchers See-To and Ho (2016) are fixed values, whereas privacy risk could create a loss from potential identity theft, which is an outcome that is difficult to predict as far as the level of impact to a person's life.

Another contribution of this study was to provide further proof for to triangulate the notional monetary value of privacy risk by comparing the results from other studies, i.e., Hann et al. (2007) and See-To and Ho (2016) (see Table 4). The figures obtained in this study are very close to those reported by See-To and Ho (2016), and are within the order of the magnitude suggested by the study by Hann et al. (2007). The comparison between the findings from this study and two other published researches provide researchers and practitioners more ideas about how customers value their privacy.

[Place Table 4 near here]

Limitations and Future Research Directions

As Gemünden (1985) suggested, consumers' reactions towards perceived risks are related to the levels of perceived risks and their tolerated risks. Users will have different reactions when the perceived risks are higher or lower than their tolerated risk levels. As the RFID-based E-payment card system that was investigated in this study was designed for micro-payment services, one can assume that the result is showing the consumers' reaction towards perceived risks, when the perceived risks are lower than the tolerated risk levels. Therefore, the authors suggest that further research should be conducted to study the scenario where consumers are facing perceived risk levels that are higher than their tolerated risk levels, such as using the E-payment service system to pay for big-ticket items.

As the authors recruited subjects to participate in this online survey through an E-government website, they were active users. As the aim of this research was to study the online consumer behaviour of using E-payment services, the authors are of the opinion that it is more appropriate to use online recruitment to attract active Internet users to participate in this survey, instead of recruiting subjects through an offline paper survey or telephone interviews, which may offer a better outreach of the population. This is to avoid recruiting users who do possess the online purchasing experience needed to participate in the survey.

The authors also anticipate that this research will bring insights to researchers in conducting similar research in different countries, which are using similar types of technology (Tan and Tan 2012). For example, Japan is using similar technology in its micro-payment and transportation market, i.e., the Suica Card System (Amoroso and Magnier-Watanabe 2012; Matsumura and Kiriya 2015). Therefore, the findings of this study may be applicable to the Suica Card System, as well. Future research of conducting further analysis on the risk propensity issues of using these types of RFID card systems in multiple countries would also be a possible extension of this research area.

Conclusion

This study was motivated by an earlier study reported by Hann et al. (2007) for studying the notional monetary value of privacy risk. The authors developed a new method to study this issue and noted that it could be used to obtain the notional monetary value of privacy risk, as well as the difference in risk attitude between two groups of users, termed “risk aversion.” This study provides a new method to explore this issue and provides insight for practitioners to develop new E-payment services for users that can encourage them to use a more convenient, yet a slightly more risky, type of payment service.

REFERENCES

Abramovici, M., and Bancel-Charensol, L. 2004. How to take customers into consideration in service innovation projects. *Service Industries Journal* 24 (1): 56–78.

Al-Khalaf, E., and Choe, P. 2020. Increasing customer trust towards mobile commerce in a multicultural society: A case of Qatar. *Journal of Internet Commerce* 19 (1): 32–61.

Amoroso, D., and Magnier-Watanabe, R. 2012. Building a research model for mobile wallet consumer adoption: The case of Mobile Suica in Japan. *Journal of Theoretical and Applied Electronic Commerce Research* 7 (1): 94–110.

Bauer, R.A. 1960. Consumer behavior as risk-taking. In Hancock, R.S. (Ed.), *Dynamic Marketing for a Changing World*, American Marketing Association, Chicago, IL, pp. 389–398.

Bergendahl, G., and Lindblom, T. 2007. Pricing of payment services: A comparative analysis of paper-based banking and electronic banking. *Service Industries Journal* 27 (6): 687–707.

Bergström, A. 2015. Online privacy concerns: A board approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior* 53: 419–426.

Bhatnagar, A., Misra, S., and Rao, H.R. 2000. On risk, convenience, and Internet shopping behavior. *Communications of the ACM* 43 (11): 98–105.

Carow, K.A., and Staten, M.E. 1999. Debit, credit, or cash: Survey evidence on gasoline purchases. *Journal of Economics and Business* 51 (5): 409–421.

Cazier, J.A., Jensen, A.S., and Dave, D.S. 2008. The impact of consumer perceptions of information privacy and security risks on the adoption of residual RFID technologies. *Communications of the Association for Information Systems* 23: Article 14.

Chakravorti, S. 2003. Theory of credit card networks: A survey of the literature. *Review of Networked Economics* 2 (2): 50–68.

Chang, M.K., Cheung, W., and Lai, V.S. 2005. Literature derived reference models for the adoption of online shopping. *Information & Management* 42 (2): 543–559.

Chang, M.-L., and Wu, W.-Y. 2012. Revisiting perceived risk in the context of online shopping: An alternative perspective of decision-making styles. *Psychology & Marketing* 29 (5): 378–400.

Chen, J.Q., Zhang, R., and Lee, J. 2013. A cross-culture empirical study of M-commerce privacy concerns. *Journal of Internet Commerce* 12 (4): 348–364.

Chiu, D.K.W., Leung, H.F., and Lam, K.M. 2009. On the making of service recommendations: an action theory based on utility, reputation, and risk attitude. *Expert Systems with Applications* 36 (2P2): 3293–3301.

Clarke III, I., and Flaherty, T.B. 2008. RFID and consumer privacy. *Journal of Internet Commerce* 7 (4); 513–527.

Featherman, M.S., and Wells, J.D. 2010. The intangibility of e-services: Effects of perceived risk and acceptance. *Database for Advances in Information Systems* 41 (2): 110–131.

Gemünden, H.G. 1985. Perceived risk and information search: A systematic meta-analysis of the empirical evidence. *International Journal of Research in Marketing* 2 (2): 79–100.

Hann, I.-H., Hui, K.-L., Lee, S.-Y.T., and Png, I.P.L. 2007. Overcoming online information privacy concerns: An Information-Processing theory approach. *Journal of Management Information Systems* 24 (2): 13–42.

Hirschprung, R., Toch, E., Bolton, F., and Maimon, O. 2015. A methodology for estimating the value of privacy in information disclosure systems. *Computers in Human Behavior* 61: 443–453.

Ho, H.C., and Awan, M.A. 2019. The gender effect on consumer attitudes toward payment methods: The case of online Chinese customers. *Journal of Internet Commerce* 18 (2): 141–169.

Ho, S.S.M., and Ng, V.T.F. 1994. Customers' risk perceptions of electronic payment systems. *International Journal of Bank Marketing* 12 (8): 26–38.

Holt, C.A., and Laury, S.K. 2002. Risk aversion and incentive effects. *American Economic Review* 92 (5): 1644–1655.

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

Hong, W., and Thong, J.Y.L. 2013. Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly* 37 (1): 275–298.

Hossain, M.A., and Dwivedi, Y.K. 2014. What improves citizen's privacy perceptions toward RFID technology? A cross-country investigation using mixed method approach. *International Journal of Information Management* 34 (6): 711–719.

Kahneman, D., and Tversky, A. 1979. Prospect theory: An analysis of decision under risk. *Econometrica* 47 (2): 263–291.

Kazan, E., and Damsgaard, J. 2016. Towards a market entry framework for digital payment platforms. *Communications of the Association for Information Systems* 38: Article 37.

Kim, C., Tao, W., Shin, N., and Kim, K.-S. 2010. An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research & Applications* 9 (1): 84–95.

Kim, D.J., Ferrin, D.L., and Rao, H.R. 2008. A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems* 44 (2): 544–564.

Lai, J.-Y. (2014). E-SERVCON and E-Commerce success: Applying the DeLone & McLean model. *Journal of Organizational and End User Computing* 26 (3): 1–22.

Lee, J.-E. R., Rao, S., Nass, C., Forssell, K., and John, J.M. 2012. When do online shoppers appreciate security enhancement efforts? Effects of financial risk and security level on evaluations of customer authentication. *International Journal of Human-Computer Studies* 70 (5): 364–376.

Liao, C., Liu, C.-C., and Chen, K. 2011. Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. *Electronic Commerce Research & Applications* 10 (6): 702–715.

Liu, C., and Forsythe, S. 2010. Sustaining online shopping: Moderating role of online shopping motives. *Journal of Internet Commerce* 9 (2): 83−103.

Liu, L., Zhu, H., and Huang, Z. 2011. Analysis of the minimal privacy disclosure for web services collaborations with role mechanisms. *Expert Systems with Applications* 38 (4): 4540–4549.

Martins, C., Oliveira, T., and Popovič, A. 2014. Understanding the Internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. *International Journal of Information Management* 34 (1), 1–13.

Matsumura, K., and Kiriya, M. 2015. Condition-based maintenance of the ticket-issuing and ticket gate equipment. In: *Proceedings of International Symposium on Seed-up and Service Technology for Railway and Maglev Systems: STECH 2015*.

Nicolaou, A.I., and McKnight, D.H. 2006. Perceived information quality in data exchanges: Effects of risk, trust, and intention to use. *Information Systems Research* 17 (4): 332–351.

Ogawara, S., Chen, J.C.H., and Chong, P.P. 2002. Mobile commerce: The future vehicle of E-payment in Japan? *Journal of Internet Commerce* 1 (3): 29−41.

PayPal. 2016. PayPal and Mastercard expand partnership to benefit consumers, merchants and financial institutions. https://investor.paypal-corp.com/releasedetail.cfm?ReleaseID=987807 (accessed August 1, 2019).

PayPal. 2017. PayPal reports fourth quarter and full year 2016 results. https://investor.paypal-corp.com/releasedetail.cfm?ReleaseID=1009339 (accessed August 1, 2019).

Pavlou, P.A., and Gefen, D. 2004. Building effective online marketplaces with institutional-based trust. *Information Systems Research* 15 (3): 37–59.

Peter J.P., and Ryan, M.J. 1976. An investigation of perceived risk at the brand level. *Journal of Marketing Research* 13 (2): 184–188.

Robinson, S.C. 2017. Self-disclosure and managing privacy: Implications for interpersonal and online communication for consumers and marketers. *Journal of Internet Commerce* 16 (4): 385–404.

Ruiz-Martínez, A. 2015. Towards a Web payment framework: State-of-the-art and challenges. *Electronic Commerce Research & Applications* 14 (5): 345–350.

Rysman, M. 2007. An empirical analysis of payment card usage. *Journal of Industrial Economics* 55 (1): 1–36.

See-To, E.W.K., and Ho, K.K.W. 2016. A study on the impact of design attributes on E-payment service utility. *Information & Management* 53 (5): 668–681.

Siyal, A.W., Ding, D., and Siyal, S. 2019. M-banking barriers in Pakistan: A customer perspective of adoption and continuity intention. *Data Technologies and Applications* 53 (1): 58–84.

Stone, R.N., and Grønhaug, K. 1993. Perceived risk: Further considerations for the marketing discipline. *European Journal of Marketing* 27 (3): 39–50.

Tan, W.-K., and Tan, Y.-J. 2012. Transformation of smart-card-based single-purpose e-micropayment scheme to multi-purpose scheme: A case study. *Expert Systems with Applications* 39 (3): 2306–2313.

Tsai, J.Y., Egelman, S., Cranor, L., and Acquisti, A. 2011. The effect of online privacy information on purchase behavior: An experimental study. *Information Systems Research* 22 (2): 254–268.

Trivedi, J. (2019). Examining the customer experience of using banking chatbots and its impact on brand love: The moderating role of perceived risk. *Journal of Internet Commerce* 18 (1): 91−111.

Tsai, W.-H., Huang, B.-Y., Liu, J.-Y., Tsaur, T.-S., and Lin, S.-J. 2010. The application of Web ATMs in e-payment industry: A case study. *Expert Systems with Applications* 37 (1): 587–597.

Tversky, A., and Kahneman, D. 1981. The framing of decisions and the psychology of choice. *Science* 211 (4481): 453–458.

Weber, E.U., Blais, A.-R., and Betz, N.E. 2002. A domain-specific risk-attitude scale: Measuring risk perceptions and risk behaviors. *Journal of Behavioral Decision Making* 15 (4): 263–290.

Yang, Q., Pang, C., Liu, L., Yen, D.C., and Tarn, J.M. 2015. Exploring consumer perceived risk and trust for online payment: An empirical study in China's younger generation. *Computers in Human Behavior* 50: pp. 9–24.

Zhang, X., and Prybutok, V. 2003. Factors contributing to purchase intentions on the Internet. *Journal of Internet Commerce* 2 (1): 3–18.

Zinman, J. 2009. Debit or credit? *Journal of Banking and Finance* 33 (2): 358–366.

APPENDIX A: Measurement Items for Privacy Risk and Overall Risk.

Privacy Risk:

(1) What is the chance that processing online payment using your credit card will cause a potential loss of control over personal information, such as when information about you is used without your knowledge or permission? (1 = Risk free; 9 = Extremely Risky).

(2) What are the chances that processing online payment using your RFID Card will cause a potential loss of control over personal information, such as when information about you is used without your knowledge or permission? (1 = Risk free; 9 = Extremely Risky).

Overall Risk:

(1) Overall, how risky is processing online payment using your credit card? (1 = Risk free; 9 = Extremely Risky).

(2) Overall, how risky is processing online payment using your RFID Card? (1 = Risk free; 9 = Extremely Risky).

APPENDIX B: Correlation Matrix

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
(1) Gender	1							
(2) Age	–0.120	1						
(3) Education Level	–0.109	0.044	1					
(4) Average Personal Income	–0.155	0.363	0.411	1				
(5) Privacy Risk (Credit Card)	0.005	0.004	–0.015	–0.020	1			
(6) Privacy Risk (RFID Card)	0.080	–0.040	0.093	0.008	0.218	1		
(7) Overall Risk (Credit Card)	0.058	–0.026	–0.068	–0.057	0.677	0.133	1	
(8) Overall Risk (RFID Card)	0.087	–0.049	0.078	0.011	0.117	0.711	0.216	1

TABLE 1. Definition of Six Dimensions of the Perceived Risk of using the E-payment Service.

Dimension of perceived risk	Definition
Financial risk	Consumer assessment of potential financial losses because of potential Internet fraud
Performance risk	Consumer assessment of potential performance problems, malfunctioning, transaction processing errors, reliability and/or security problems, that cause the E-payment service to not perform as expected.
Privacy risk	Consumer assessment of potential losses to the privacy and confidentiality of their personal identifying information and that E-payment usage exposes them to potential identity theft.
Psychological risk	Consumer assessment of potential losses to their self-esteem, peace of mind or self-perception (ego) because of worrying, feeling frustrated, or foolish a result of using E-payment service.
Social risk	Consumer assessment of potential losses to their perceived status in their social group as a result of using an E-payment service. The assessment of the probability that consumers believe that they will look foolish to important others.
Time risk	Consumer assessment of potential losses to convenience, time and effort caused by wasting time researching, purchasing, setting up, switching to and learning how to use the E-payment service.

Note: The information on this table is extracted from Table 1 of Featherman and Wells (2010).

TABLE 2. Demographic Data.

	Users of anonymous card (i.e., L-type)			Users of personalized card (i.e., H-type)			Overall Samples		
	Male (N = 556)	Female (N = 683)	Overall (N = 1,239)	Male (N = 313)	Female (N = 206)	Overall (N = 519)	Male (N = 869)	Female (N = 889)	Overall (N = 1758)
General demographic									
Average age	30.6	28.7	29.6	33.6	32.9	33.3	31.7	29.7	30.7
Average annual personal income (US$)	$13,084 ($12,356)	$10,613 ($11,460)	$11,722 ($11,943)	$152,396 ($92,515)	$19,538 ($12,352)	$17,716 ($12,254)	$15,409 ($12,580)	$11,617 ($11,809)	$13,491 ($12,339)
Frequencies of online shopping per year	5.28 (9.72)	4.81 (9.88)	5.02 (9.81)	7.94 (12.44)	5.00 (8.69)	6.78 (11.19)	6.24 (10.85)	4.85 (9.62)	5.54 (10.26)
Education background									
High school or below	220 (39.6%)	301 (44.1%)	521 (42.1%)	79 (25.2%)	80 (38.8%)	159 (30.6%)	299 (34.4%)	381 (42.9%)	680 (38.7%)
College	304 (54.7%)	360 (52.7%)	664 (53.6%)	202 (64.5%)	115 (55.8%)	317 (61.1%)	506 (58.2%)	475 (53.4%)	981 (55.8%)
Graduate school	32 (5.8%)	22 (3.2%)	54 (4.4%)	32 (10.2%)	11 (5.3%)	43 (8.3%)	64 (7.4%)	33 (3.7%)	97 (5.5%)

Note: Numbers in parenthesis for the number of average annual personal income and frequencies of online shopping per year are standard deviations.

Table 3. Responses from Our Subjects

	Personalized Card User (H-Type)	Anonymous Card User (L-type)
Online credit card service		
Perceived risk	6.3545 (1.7927)	6.6796 (1.1849)
Perceived privacy risk	6.7919 (1.9190)	6.9266 (1.9506)
Online RFID-based E-payment service card service		
Perceived risk	5.5819 (2.0759)	5.2478 (2.1673)
Perceived privacy risk	5.9152 (2.2568)	5.4689 (2.3820)

Note: Numbers in parenthesis are standard deviations.

Table 4. Notional Monetary Value of Privacy Risk

	Notional Monetary Value of Privacy Risk	Notes
Current Study	US$134.16 – $268.32	From a laboratory experiment involving 1,758 subjects based on a real E-payment service.
Hann et al. (2007)	US$30.49 – $44.62	From a laboratory experiment involving 268 subjects based on a hypothetical E-commerce Website.
See-To and Ho (2016)	Payment with Identity: US$94.13 – $114.36 Online Data Transfer for Payment US$297.36 – US$682.44	From a laboratory experiment involving 1,795 subjects based on a real E-payment service. Figures calculated from the results reported by See-To and Ho (2016).