FinTech and Contactless Payment - Help or Hindrance? The Role of Invasion of Privacy and Information Disclosure

Ali Abdallah Alalwan
Department of Management and Marketing, College of Business and Economics, Qatar University, P.O. Box - 2713, Doha, Qatar
aalalwan@qu.edu.qa

Abdullah M. Baabdullah
Department of Management Information Systems, Faculty of Economics and Administration, King Abdulaziz University, Jeddah, Saudi Arabia
baabdullah@kau.edu.sa

Mutaz M. Al-Debei [a, b]
[a] Dean of Business School, Department of Business Analytics, Business School Al-Ahliyya Amman University
Email: mdebei@ammanu.edu.jo

[b]Department of Management Information Systems, Business School, The University of Jordan, Jordan

Ramakrishnan Raman
Symbiosis Institute of Business Management, Pune
& Symbiosis International (Deemed University), Pune, India
Email: director@sibmpune.edu.in

Hitmi Khalifa Alhitmi
Department of Management and Marketing, College of Business and Economics, Qatar University, P.O. Box - 2713, Doha, Qatar
Email: Halhitmi@qu.edu.qa

Amjad Abu-ElSamen
Zayed University, Department of Marketing and Entrepreneurship, Abu Dhabi, UAE
amjad.abuelsamen@zu.ac.ae

Yogesh K Dwivedi [a, b]
[a]Digital Futures for Sustainable Business & Society Research Group, School of Management, Swansea University, Bay Campus, Fabian Bay, Swansea, SA1 8EN, Wales, UK
Email: y.k.dwivedi@swansea.ac.uk

[b] Department of Management, Symbiosis Institute of Business Management, Pune & Symbiosis International (Deemed University), Pune, Maharashtra, India

Abstract

Purpose – There is always a need to discover how a paradox between a customer's desire for a more personalized experience and their privacy and security concerns would shape their intention to continue using contactless payment methods. However, personalization–privacy paradox has not been well-covered over the area of contactless payment. Therefore, this study aims to empirically examine the impact of personalization–privacy paradox on the customers' continued intention to use contactless payment.

Design/methodology/approach – The empirical part of the current study was conducted in Saudi Arabia by collecting the primary data using online questionnaire from a convenience sample size of 297 actual users of contactless payment methods.

Findings – Based on structural equation modelling (SEM), personalization and privacy invasion were approved to significantly impact perceived value of information disclosure. Strong causal associations were confirmed between perceived severity; structural assurance and response cost with privacy invasion. Finally, both perceived value of information disclosure and privacy invasion significantly predict continued intention.

Research limitations/implications – There are other important factors (i.e. technology interactivity; technology readiness; social influence; trust; prior experience; etc) were not tested in the current study. Therefore, future studies would pay more attention regarding the impact of these factors. The current study data was also collected using a convenience sample of actual users of contactless payment methods. Therefore, there is a concern regarding the generalizability of the current study results to other kind of customers who have not used contactless payment.

Originality/value – This study has integrated both personalization–privacy paradox and protection motivation theory in one model. Accordingly, the current study has a value by providing new and full picture about new kinds of inhibitors and enablers of customers' continued intention to keep using contactless payment. Furthermore, personalization–privacy paradox has not been fully examined over the related area of Fintech and contactless payment in general. Therefore, this study was able to extend the theoretical horizon personalization–privacy paradox to new area (i.e. contactless payment) and new cultural context (Saudi Arabia).
Keywords: Fintech; contactless payment; personalization–privacy paradox; information disclosure; continued intention.

Paper type: Research paper

1. Introduction

Worldwide, many businesses (i.e. Visa; MasterCard; Apple; and Samsung) showed an unparalleled interest in providing innovative financial solutions to their customers by relying on the contemporary boom in Fintech (i.e. Contactless payment) (Al-Okaily et al., 2022; Al-Sharafi et al., 2021; Baabdullah et al., 2019; Karjaluoto et al., 2020; Trütsch, 2020; Lee and Pan, 2022; Moghavvemi et al., 2021). Contactless payment is among the most common

examples of the FinTech systems that have received a considerable attention of business organizations especially in the light of the increase in the rate of using smart phones for other purposes such as online shopping, payment, and banking (Al-Qudah et al., 2022; Karjaluoto et al., 2019; Kalia et al., 2022; Trütsch, 2020). Indeed, contactless payment presents high tech and innovative financial solutions for the most of the customers' problems (Bounie and Camara, 2020; Nilsson, 2021) that have increasingly contributed to improving the consumer experience and the level of financial performance alike (Bounie and Camara, 2020; Nilsson, 2021). Thus, customers worldwide seem to be motivated to use or continue using contactless payment. For example, the number of contactless payment (i.e. Proximity mobile payment) users reached about 1.18 billion by 2020 worldwide and this number is expected to reach about 1.35 billion users by the end of 2022 (eMarketer, 2021).

The concept of contactless payment has been increasingly used by practitioners as a more secured payment method at brick-and-mortar stores and without the customer having to touch anything with their hand (Karjaluoto et al., 2019; Bounie and Camara, 2020; Nilsson, 2021). Technically, by having Near Field Communication (NFC) technology, the customer can make the payment by keeping his/her smartphone card (i.e. mobile payment near the payment terminal)/ debit/ and credit card without having to enter a PIN code (Karjaluoto et al., 2019). Contactless payment could be noticed in different forms such as Apple Pay, Visa Contactless, Samsung Pay, MasterCard PayPass, Android Pay, and Google pay (Lacmanović et al., 2010; Karjaluoto et al., 2019).

In fact, customers are more likely to have a smooth, flexible, convenience, personalised and easy experience in the payment process compared to before (Karjaluoto et al., 2019; Gerpott and Meinert, 2017; Lacmanović et al., 2010; Shishah and Alhelaly, 2021; Zakonnik et al., 2018; Zhao et al., 2019). Thus, personalization would be considered as one of the key driver of the customer adoption and satisfaction toward contactless payment. Personalization is referred to the unique features of emerging systems (i.e. contactless payment) that allow customers to modify products and services based on their preferences and behaviours (i.e. Alalwan et al., 2020). However, a high level of personalization requires a full understanding of customers' behaviour and preferences. Technically, personalization would be considered in different aspects, such of that Customer are empowered at the beginning to select contactless payment as one of payment methods available (i.e. paying cash; using visa machine; etc.). Contactless payment methods also allow customers to customise the authentication method used to have a secure payment. For example, there are several

biometric authentication methods (i.e. fingerprint scanning, facial recognition, and voice recognition) that customer can freely use any of them to have a secure payment. A high tech contactless payment allows customers to follow up the amount of their spending or any fraudulent attempt by allowing them to personalise the appropriate alert method, whether through notifications or SMS. Further, by using contactless payment, customers are able to set limits on the volume of spending, the number of executed operations, and the locations of their use. Furthermore, contactless payment methods help companies track customers' purchasing behavior and preferences, and thus there is a greater opportunity to personalise offers and discounts to better meet customer expectations.

However, there is always debate regarding the main concerns related to the customers' privacy and security especially in the light of the fact that these applications requires customers to disclose their personal and financial identity and information (Kılınç and Vaudenay, 2018; Karjaluoto et al., 2019; Chen et al., 2023). This would be attributed to the fact that customers are usually worried regarding their private and sensitive information especially these pertain to financial matters (Lee et al., 2016; Alalwan et al., 2017; Lei et al., 2022). Conceptually, "privacy concerns mainly centre on the collection of data, data errors, unauthorised access, and unauthorised secondary use of the information collected" (Vimalkumar et al., 2021, p. 5). As argued by Lei et al. (2022) recently, customer seems to be concerned regarding how his/ her information would be accessed and used as well as who has the ability to access and use his/ her information. Therefore, privacy concern has been commonly reported as key inhibitor of new systems adoption especially these enjoy with high level of personalisation and information disclosure (Baabdullah et al., 2019; Lei et al., 2022; Vimalkumar et al., 2021). In this respect, a recent study published by the Global Fintech Survey indicated that 56% of study participants clearly showed their concerns regarding aspects related to information privacy and security (World FinTech Report, 2021).

In the light of the above mentioned discussion, users of contactless payment are more likely to engage in a comparison between the desires to obtain a high level of customization and, at the same time, the concerns arising from disclosing their personal information. This, in turn, creates a persistent need to discover how such a paradox between a customer's desire for a more personalized experience and their privacy and security concerns would shape their intent to continue using contactless payment methods. Furthermore, personalization–privacy paradox has not been well-covered over the area of contactless payment (i.e. contactless payment), and accordingly, it was considered as a gap to be considered in the current study

(Karwatzki et al., 2017; Lei et al., 2022). Therefore, this study aims to empirically examine the impact of personalization–privacy paradox on the customers' continued intention to use contactless payment.

A review of the main body of literature is provided in section 2: Literature review followed by discussing the conceptual model and research hypotheses in Section 3. Section 4 explains the research methodology applied in the current study. Results are presented in Section 5. Section 6 is devoted for results discussion and theoretical and practical implications. Research conclusion is presented in Section 7.

2. Literature review

In spite of the fact that Fintech has increasingly been the focus of attention of researchers over the business and information system area, a little interest has been paid by researchers to examine the related issues of contactless payment methods. In this regard, Karjaluoto et al. (2019, p. 333) asserted that "*only a few have explored specific forms of digital payments, such as NFC-based contactless payments*". However, these limited attempts in the area of contactless payment have enlarged the current understanding regarding the related aspects that could shape the customers' behaviour and experience toward such emerging systems (i.e. Bounie and Camara, 2020; Karjaluoto et al., 2019; Trütsch, 2020; Banerjee and Sreejesh, 2021; Gupta and Narayan, 2021; Cocosila and Trabelsi, 2016; Lee and Pan, 2022; Semerikova, 2020) (see Appendix).

Conceptually, "Contactless payment" is a kind of an emerging payment methods empowered by near-field communication (NFC) technology that allow customers to securely do their payments at any retailer stores by holding the smartphone card/ debit card/ and credit card close to the point-of-sale (POS) terminal (which carries the contactless wave symbol) without having to enter a PIN code (Karjaluoto et al., 2019, p. 332). Contactless payment could be noticed in different forms such as Apple Pay, Visa Contactless, Samsung Pay, MasterCard PayPass, Android Pay, and Google pay (Lacmanović et al., 2010; Karjaluoto et al., 2019).

A careful reviewing of these research attempts leads to notice a number of themes such as customer acceptance (i.e. Bounie and Camara, 2020; Zhong et al., 2021); sustainable use (i.e. Al-Sharafi et al., 2021); consumer brand engagement (i.e. Karjaluoto et al., 2019); customer experience (i.e. Shishah and Alhelaly, 2021); cash usage and spending behaviour (i.e. See-To and Ngai, 2022; Trütsch, 2020); system authentication (i.e. Gupta and Narayan, 2021);

perceived risk (i.e. Cocosila and Trabelsi, 2016); pandemic effect (i.e. Daragmeh et al., 2021; Otterbring and Bhatnagar, 2022); and usage barriers (i.e. Semerikova, 2020).

Further, several factors have been considered by prior researches of contactless payment. For example, Zhong et al. (2021) proposed an extended framework based on Technology Acceptance Model (TAM) and other factors (Enjoyment; innovativeness; facilitating conditions; and coupon availability). The empirical part of Zhong's et al. (2021) study was conducted in South Korea and their statistical findings largely supported the role of perceived usefulness and ease of use on the customer's attitudes, which in turn, predicts the customers' intention to use contactless payment (i.e. facial recognition payment). Zhong et al. (2021) were also able to empirically approve the significant impact of perceived enjoyment on both customers' attitudes and intention to use facial recognition payment. Coupon availability was another factor approved by Zhong et al. (2021) to have a significant impact on usefulness and intention to use. However, according to Zhong et al. (2021), innovativeness and facilitating conditions only predict perceived usefulness. In their study to explore the key factors predicting the sustainable use of contactless mobile payment, Al-Sharafi et al. (2021) considered several theoretical foundations (i.e. the protection motivation theory; the expectation-confirmation model; and trust model). The yielded results of Al-Sharafi's et al. (2021) study showed that customer's continued intention to keep using contactless payment is strongly influenced by the role of expectation confirmation; perceived usefulness; customer satisfaction; self-efficacy; response cost; perceived severity; vulnerability; and trust. Network speed, ability to recognize biometrics, problems related to phone battery and privacy and security factors all were proposed and empirically tested by Semerikova (2020) as key barriers hindering the likelihood of customers' usage of Mobile contactless payment. Semerikova's (2020) empirical results approved these barriers which should be taken into account to accelerate the likelihood of customers' usage of Mobile contactless payment.

Brand engagement model was integrated by Karjaluoto et al. (2019) with the extended Unified Theory of Acceptance and Use of Technology (UTAUT2) to predict the Finnish customer's continued intention to use contactless payment. Karjaluoto et al. (2019) have also argued the negative impact of perceived risk. Their empirical results largely supported the positive impact of brand engagement on the customer's continued intention to use contactless payment. From UTAUT2 model, three factors (performance expectancy; effort expectancy; habit; and facilitating conditions) were approved by Karjaluoto et al. (2019) to have a significant impact on continued intention to use contactless payment. On the other hand,

perceived risk was noticed to have a negative impact on the continued intention. So as to examine the impact of COVID-19 pandemic, Daragmeh et al. (2021) integrated the technology acceptance model (TAM) with perceived COVID-19 risk to validate the key factors predicting Generation X's intention to use Mobile payment methods (contactless payment) in Hungary. Their empirical results assured the significant role of perceived usefulness; subjective norms; and perceived COVID-19 risk on the Generation X's intention to use mobile contactless payment. Similar to Daragmeh et al. (2021), Otterbring and Bhatnagar (2022) have recently explored the impact of COVID-19 pandemic on the customers' payment method preferences (cash or contactless payment). Otterbring and Bhatnagar (2022) showed that customers are more likely to prefer contactless payment method than using cash due to their concerns of transmission of COVID-19 infection by touch.

In different way, Cocosila and Trabelsi (2016) empirically argued the perceived value in light of the contrasts between drivers (as gains) and inhibitors (as cost). In details, three kinds of utilities: hedonic; social; and cognitive were proposed by Cocosila and Trabelsi (2016) as key gains stimulating perceived value of using contactless payment. According to Cocosila and Trabelsi (2016), perceived risk was treated as a kind of cost and encompass five dimensions : time; psychological; privacy; and social. Their results indicated that while perceived value of using contactless payment is strongly accelerated by three kinds of gains (hedonic; social; and cognitive, perceived value is inhibited by the role of perceived risk. Cocosila and Trabelsi (2016) added that perceived value is a contributor of the customer intention to use contactless payment. See-To and Ngai (2019) have tested the impact of payment method (i.e. traditional credit cards; contactless smart cards; and cash) on the customer' expenditure behaviour. In the line with what has been reached by See-To and Ngai (2019), payment method which enjoys with more convenience, security, and preciseness is positively associated with the customers' expenditure behaviour. In different words, spending behaviour was noticed to be the high among those customers who use contactless smart cards. This was attributed by See-To and Ngai (2019) to the unique features that contactless smart cards could have in terms of convenience, security, and preciseness.

Even though these few research attempts have accelerated the current understanding regarding the key aspects that shape the customer's reaction and behaviour toward contactless payment, there is still a need to see other inhibitors and enablers that could predict the customer's intention and behavior toward contactless payment systems. As discussed earlier

in the introduction part, it would be useful to explore how the paradox between a customer's desire for a more personalized experience and their privacy and security concerns would shape their intent to continue using contactless payment methods. Further discussion regarding the personalization–privacy paradox is provided in the forthcoming subsection.

2.1 Personalization–privacy paradox

Personalization–privacy paradox was selected as a as a theoretical base of the current study model (Karwatzki et al., 2017; Lei et al., 2022). The "personalization-privacy paradox" has been one of the most common models referred by researchers in the IS and digital marketing area to understand the pros and cons of personalization (Lei et al. 2022; Cloarec et al., 2022). In fact, personalization is not something for free to be given to the customer but rather there is a cost should be paid in terms of personal information disclosure. Therefore, privacy concerns have always presented the dark side resulted from a higher level of personalization, which later was the most important disincentive for consumers to enjoy a positive experience in using personalized service and technology (i.e. contactless payment) (Lei et al. 2022; Cloarec, 2020; Sutanto et al., 2013; Lee and Cranage, 2011). In fact, as mentioned above, Personalization–privacy paradox has not been fully examined by prior studies of contactless payment (see Appendix). Therefore, this study found it is important to explore how such a paradox between a customer's desire for a more personalized experience and their privacy and security concerns would shape their intent to continue using contactless payment methods.

2.2 Protection motivation theory

Protection Motivation Theory (PMT) was proposed by Rogers (1983) to explain people beliefs would impact their perception and behaviour over the sociology and health fields (Rippetoe and Rogers, 1987; Milne et al., 2000). Originally, cognitive and value perspectives were considered in proposing protection motivation theory so as to address fear appeals (Ifined, 2012). Protection motivation model also enjoys with a high predicative validity as reported by Anderson and Agarwal (2010). This would be returned to the both initiate threat and coping appraisals are considered in protection motivation model (i.e. Scarpa and Thiene, 2011; Williams et al., 2015; Vance et al., 2015; Al-Sharafi et al., 2021). As for the current study, there is also a need to look at the effective mechanisms that help customers to overcome obstacles pertaining to his/ her privacy concerns. Thus, protection motivation theory will also be considered in the current study model so as to provide a comprehensive

picture regarding the main factors that could shape the customers' privacy concerns, and accordingly, hindering or contributing to the adoption of FinTech (i.e. Contactless payment). According to protection motivation theory, perceived severity; response cost; self-efficacy; and perceived structural assurance will be proposed as key factors predicting Invasion of privacy (Vance et al., 2012; Williams et al., 2015; Li, 2012; Ifinedo, 2012).

3. Conceptual Model and research hypotheses

As seen in Figure 1, eight factors have been proposed in the current study model. Invasion of privacy was expected to be influenced by the role of perceived structural assurance; self-efficacy; and perceived severity. Invasion of privacy, in turn, would have a direct impact on perceived value of information disclosure and continued intention to use contactless payment. Perceived personalization was proposed to have a sole impact on perceived value of information disclosure. More justifications regarding the casual paths proposed in the current study will be presented in the forthcoming subsections.

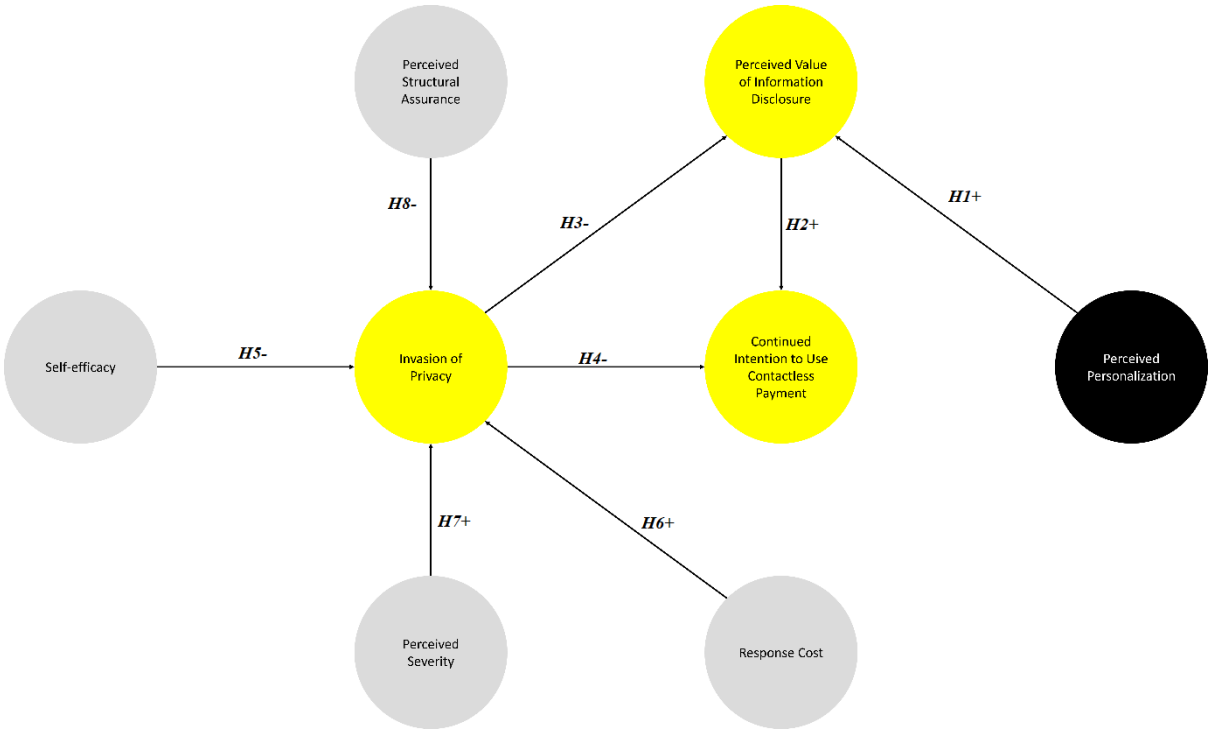

Figure 1: Conceptual Model (Source: Adapted from Lei et al., 2022; Vance et al., 2012)

3.1 Perceived personalization

Personalization is referred to the unique features of emerging systems (i.e. contactless payment) that allow customers to have a high personalized content, experience, products, and services based on their preferences and behaviours (i.e. Alalwan et al., 2020; Lee et al., 2023). Personalization in contactless payment would also be noticed by providing different

touchless payment methods (i.e. contactless payment card; Mobile contactless payment [i.e. Apple pay; Google pay]; payment by code) and allowing customers to freely select among them. Customers would also freely identify the limit that he/ she could pay using contactless payment method. Further, Personalized contactless payment empower consumers to freely choose the authentication method for payment [i.e. insert password; phone number; one time password (OTP); biometric authentication (i.e. Iris recognition, Retina recognition, Face recognition, and Voice recognition)]. The consumer can specify the spatial and temporal space for the use of contactless payment, which represents more aspects of personalization.

Accordingly, personalization would help customers to have high quality of contactless payment services as they want and expect. This, in turn, helps customers to attain a positive experience in using contactless payment. However, a high level of personalization requires a full understanding of customers' behaviour and preferences. Thus, it would be argued that if customers are not sufficiently convinced of the quality and importance of the personalised services, it may be difficult for them to place value on disclosing personal information or sacrificing their privacy (Lee and Rha, 2016; Lei et al., 2022; Pal et al., 2020; Kumar et al., 2022). In other words, customer who positively values personalization and see such customized services more useful and important for their experience, is more likely to positively value of information disclosure (Pal et al., 2020). In this regard, one of the unique characteristics of contactless payment is the value of personalization that motivates the consumer to take a risk and disclose his/ her private information (Xu et al., 2011; Lee and Rha, 2016; Pal et al., 2020). Such proposition has been empirically approved by Xu et al. (2011) and more recently Pal et al. (2020) who supported the impact of personalization on the perceived value of information disclosure. Thus, this study proposes that:

H1: Perceived personalization will positively impact the customers' perceived value of information disclosure.

3.2 Perceived value of information disclosure

Customer is more likely to be engaged in trade-off process between the cost of disclosing personal information and benefits of high personalized services (Cloarec et al., 2022; Lee and Rha, 2016; Xu et al., 2011). The main consequence of such trade-off process yields the cumulative effect of consumer concerns and perceived benefits, which is termed as perceived value (Xu et al., 2011; Cloarec et al., 2022; Lee and Cranage, 2011; Marriott et al., 2017). In the current study, it has been followed what was proposed by Xu et al. (2011) regarding perceived value of information disclosure construct. In details, Xu et al. (2011, p. 44) defined

perceived value of information disclosure as "the individual's overall assessment of the utility of information disclosure based on perceptions of privacy risks incurred and benefits received". In the line with what has been proposed by Xu et al. (2011) and Pal et al. (2020), the more customers expect a higher value of disclosing personal information, the more they will be motivated to keep using contactless payment. The relationship between perceived value of information disclosure and behavioural intention was supported by Xu et al. (2011) in the context of location-aware marketing. Pal et al. (2020) also approved the significant impact of perceived benefits of personal information disclosure on the customer's continued intention to use Voice Assistants. Thus, this study proposes that:

H2: Perceived value of information disclosure will positively impact the customers' continued intention to use contactless payment.

3.3 Privacy Invasion

According to Choi et al. (2009, p. 678), privacy invasion would be defined as the extent to which customer perceives a risk that his/ her private and personal information would be illegally shared outside the agreed limits, and thus, the consumer is exposed to an embarrassing situation involuntarily. As discussed before, a high level of personalization requires customer to disclose a large an amount of personal information. However, a customer who has a high degree of privacy sensitivity will refrain more from disclosing his/ her personal information to obtain personalized services (Bolderdijk et al., 2013; Hughes et al., 2016; Lee and Cranage, 2011; Sandhu et al., 2023; Xu et al., 2011). Further, a side effect of clients' fears of invasion privacy is a reduced level of satisfaction or even perceived value for services that require as much disclosure of private information as in the case of highly personalized services (Lei et al., 2022; Aguirre et al., 2015). Xu et al. (2011) argued that customers who had a bad experience of privacy invasion are more likely to perceive a high level of perceived risk and underestimate the value of personalised services. Privacy invasion has been recently proven by Lei et al. (2022) to have a negative role in hindering the customers' willingness to adopt personalized services. Thus, this study proposes that:

H3: Privacy invasion will negatively impact the customers' perceived value of information disclosure.
H4: Privacy invasion will negatively impact the customers' continued intention to use contactless payment.

3.4 Self-efficacy

In the context of personalization and privacy services, Self-efficacy is returned to the extent of how much the user of contactless payment is able to secure his/her personal information

and privacy (Chen and Chen, 2015; Lee and Rha, 2016; Faqih, 2013). A careful reviewing the main body of literature leads to notice that customers, who enjoy with high level of self-efficacy, are less likely to have privacy concerns as well as they are more willing to disclose their personal information to enjoy with high level of personalization (Al-Emran et al., 2020; Daragmeh et al., 2021; Lee and Rha, 2016; Sundar and Marathe, 2010). This thought was empirically validated by Lee and Rha (2016) who supported the significant role of self-efficacy in mitigating privacy risk in the location-based applications. A study conducted by Vance et al. (2012) empirically approved the impact of self-efficacy on the extent of how much system user comply security policy to protect the confidential information. Over the context of contactless payment, Al-Sharafi et al. (2021) supported the positive impact of self-efficacy on the customer's continued intention to keep using mobile contactless payment. Al-Emran et al. (2020) also supported the positive role of self-efficacy in enhancing the behavioural intention to use smartwatches among university students. Accordingly, this study proposes that:

H5: Self-efficacy will negatively impact the invasion privacy pertaining to using contactless payment.

3.5 Response cost

According to Protection Motivation Theory, response cost is one of the main dimensions that determine the technology user's ability to cope with any risk or invasion privacy (Vance et al., 2012). Conceptually, response costs would be defined as all kinds of costs (i.e. money, time, efforts, complexity; side effect) (i.e. Scarpa and Thiene, 2011; Al-Sharafi et al., 2021). To put it differently, customers, who perceive a high level of response costs, are more likely to perceive using contactless payment contactless as source of threats of their own privacy, and therefore, they will be less motivated to keep using such emerging payment systems in future. The significant role of response cost has been validated by a number of studies over the digital area. For example, Vance et al. (2012) provided further statistical evidences approving negative impact of response cost on user's intention to comply with system security policy. Al-Sharafi et al. (2021) also empirically confirmed the negative impact of response cost on the customers' continued intention to keep using mobile contactless payment. Over the higher educational area, Al-Emran et al. (2020) supported the negative impact of response cost on the intention to use smartwatches. Accordingly, this study proposes that:

H6: Response cost will positively impact the invasion privacy pertaining to using contactless payment.

3.6 Perceived severity

According to Gaube et al. (2019, p. 103), perceived severity is defined as "the assumed degree of harm arising from the negative outcome of a particular behavior". As the current study attempts to address to psychological and social burdens arsing from inability of the contactless payment system to maintain consumer privacy and information, perceive severity will be proposed as key factor accelerating invasion privacy. Indeed, there are serval negative consequences of information disclosure that would heighten the level of perceived severity such as identity theft, vulnerable to security incidents, cyberstalking, and financial and commercial fraud (e.g., Debatin et al., 2009; Walrave et al., 2012; Aharony, 2016). This is in addition to the psychological and social effects of information disclosure on the customers feeling of anxiety that their image would be negatively evaluated by others (Cameron et al., 2009).

The role of perceived severity has been commonly reported over the Fintech context as the customers, systems, and digital services are closely paired with each other (Pal et al., 2020). In fact, using contactless payment requires customers disclosing their private information or even using their biometric tag (voice or face recognition). Therefore, Contactless payment users are more vulnerable to online fraud or identity theft (Pal et al., 2020; Kamboj et al., 2022). All things considered, it would be argued that over the situation that customer perceive a high level of privacy and security concerns, customer is more likely to perceive a high level of perceive severity, and accordingly, more willing to proactively behave (i.e. Boehmer et al., 2015; Pal et al., 2020). Accordingly, this study proposes that:

H7: Perceived severity will positively impact the invasion privacy pertaining to using contactless payment.

3.7 Structural assurance

Structural assurance is more related to the extent of the availability of the technical infrastructure, mechanisms, and legal framework that guarantees the secure use of technology and prevents hacking or misuse of customers' personal information (Zhou, 2012; Park et al., 2015). Over the prior literature of Fintech, structural assurance has been commonly reported as a mechanism leveraging the users trust in the banking systems as well as relieving their concerns and risks (Aladwani and Dwivedi, 2018; Zhou, 2012). In fact, the existence of structural assurance would assure that the financial companies providing contactless payment

services are keen to maintain a high level of efficient and effective performance and a high level of transparency as well (Park et al., 2015). Therefore, it would be argued that structural assurance in the contactless payment would not only enhance the customer's trust in such emerging financial systems but also would mitigate the customer's concerns regarding the invasion of privacy. Accordingly, this study proposes that:

H8: structural assurance will negatively impact the invasion privacy pertaining to using contactless payment.

4. Methodology

The empirical part of the current study was conducted in Saudi Arabia by collecting the primary data using online questionnaire from a convenience sample size of 500 actual users of Contactless payment methods over the period started from the 1st of May 2022 to the 15th of Jun 2022. A large sample size (500) was important to increase the sample representativeness as well as to address the related issues of sampling bias. The targeting process also took into consideration the demographic differences in the study population and sought to accurately represent all groups (Bhattacherjee, 2012; Bryman, 2004). In fact, a wide range of contactless payment methods were considered in the current study such as Apple Pay, Visa Contactless, Samsung Pay, MasterCard PayPass, Android Pay, and Google pay (Lacmanović et al., 2010; Karjaluoto et al., 2019).

The eight latent constructs in the current study model were measured using scale items that have been extracted from prior literature and adapted to the nature of contactless payment methods. In details, 4 items proposed by Xu et al. (2011) and Lee and Rha (2016) were used to measure personalization. A scale of Xu et al. (2011) was also adapted to measure perceive value of information disclosure. Privacy invasion was tested using four scale items suggested by Lee and Rha (2016). Four scale items were derived from Leung and Cai (2021) to test self-efficacy. Al-Sharafi's et al. (2021) measurement items were used to test response cost and perceived severity. Three items suggested by Zhou (2012) were considered to measure structural assurance of contactless payment. Continued intention to use contactless payment was tested based on scale items suggested by Lee and Rha (2016).

All scale items were translated to the Arabic language using the back-translation method (Brislin, 1976). Further, the translated questionnaire has been reviewed and validated by panel of experts so as to assure the adequacy of these items to measure the latent constructs. Before conducting the main survey, a pilot study was conducted with a number of actual

users (35 participants) of contactless payment in Saudi Arabia. The vast majority of those participants) assured that the language of the questionnaire is clear and understandable without any complexity, and does not take long time to be completed. Cronbach's alpha values for the eight constructs were also inspected and found to be within their recommended level (> .70) (Nunnally, 1978).

Table 1: Measurement Items			
Construct		Items	Reference
Personalization	PRS1	Contactless payment can provide me with personalized deals/ads tailored to my activity context.	Xu et al. (2011)
	PRS2	Contactless payment can provide me with more relevant promotional information tailored to my preferences or personal interests.	
	PRS3	Contactless payment can provide me with the kind of deals/ads that I might like.	
	PRS4	I can get personalized information tailored to my shopping patterns.	Lee and Rha (2016)
Perceived value of information disclosure	PVD1	I think my benefits gained from the use of contactless payment can offset the risks of my information disclosure.	Xu et al. (2011)
	PVD2	The value I gain from use of contactless payment is worth the information I give away.	
	PVD3	I think the risks of my information disclosure will be less than the benefits gained from the use of contactless payment.	
Privacy invasion	PVN1	By using contactless payment, I am at the risk of infringement of my privacy.	Lee and Rha (2016)
	PVN2	By using contactless payment, I am at the risk of my personal information being excessively collected.	
	PVN3	By using contactless payment, my personal information is at the risk of being accessed by unauthorized people.	
	PVN4	By using contactless payment, my actions are at the risk of being tracked and monitored.	
Self-efficacy	SE1	I will be able to control the risk of using contactless payment.	Leung and Cai (2021)
	SE2	I know how to keep myself safe in using contactless payment.	
	SE3	I am confident that I can stay safe while using contactless payment.	
	SE4	Compared to other people, I can do protect myself very well while using contactless payment.	
Response cost	RC1	Contactless payment is expensive for making secure payments.	Al-Sharafi et al. (2021)
	RC2	I have to frequently upgrade my contactless payment for making secure payments.	
	RC3	Security incidents can slow down the contactless payment technologies performance.	
	RC4	Compliance with mobile contactless payment security policy would require a considerable investment of effort other than time.	
Perceived severity	PVR1	I believe that contactless payment is vulnerable to security incidents.	Al-Sharafi et al. (2021)
	PVR2	I believe that the productivity of contactless payment is threatened by security incidents.	
	PVR3	I believe that the profitability of contactless payment is threatened by data protection incidents.	
	PVR4	Having my personal identity stolen by the contactless payment will be a serious problem for me.	Mohamed and Ahmad (2012)
Structural assurance	STA1	I feel confident that encryption and other technological advances make it safe for me to use contactless payment.	Zhou (2012)
	STA2	I feel assured that legal and technological structures adequately protect me from payment problems on the contactless payment.	
	STA3	Internet and Wi-Fi networks are robust and safe environment in which to use contactless payment.	
Continued intention	CIN1	I intend to continue using contactless payment.	Lee and Rha (2016)
	CIN2	I intend to purchase from contactless payment in the future.	
	CIN3	I intend to recommend using contactless payment to my friends.	

5. Results

5.1 Demographic Characteristics

As reported in the methodology section, 500 questionnaires were distributed in the current study. Yet, about 297 (59.4% response rate) valid responses were captured and processed to the statistical analyses. The current sample size (297) seems to be applicable to empirically validate the current study model and research hypotheses as suggested by Kline (2005) who asserted that a study sample size ranging from 200 to 400 is considered sufficient to conduct a statistical test (i.e. Structural Equation Modelling) for a complex study model that consists of a number of variables, as is the case in the current study.

Table 2: Demographic Characteristics

Demographic Profile	Number of Participants (N= 297)	Percentage (%)
Gender		
Male	164	55.2
Female	133	44.8
Total	297	100
Age		
18-24	56	18.8
25-30	97	32.6
31-40	73	24.5
41-50	38	12.7
51-60	29	9.7
60+	4	1.3
Total	297	100.0
Monthly income (Saudi Riyals)		
Less than 1000	24	8.08
1000-4000	67	22.5
4001-8000	85	28.6
8001-14000	71	23.9
14000-20000	16	5.38
More than 20000	34	11.4
Total	297	100
Education Level		
High school	15	3.9
Diploma	36	10.2
Bachelor	142	54.3
Master	56	21.9
PhD	31	8.9
Other	17	.8
Total	297	100
Contactless payment Experience		
Less than one year	49	16.4
1-2 years	67	22.5
2-3 years	125	42.8
More than 3 years	56	18.8
Total	297	100

Table 2 shows that about 55.2% of the current study's respondents were male (55.2) while about 44.8% were female. The largest part of the current study respondents were noticed to be within age category of 25-30 (32.6%) followed by those whose age category between 31-40. Most of the participants have a monthly income raging between 4001 to 14000 Saudi Riyals. As for the educational level, the vast majority of the current sample respondents (54.3%) have a Bachelor degree and then those who have a Master degree (21.95). This study has mainly targeted the actual users of contactless payment, and therefore, most of those participants (42.8%) have a usage experience with contactless payment method ranging between 2 to 3 years (see Table 2).

5.2 Common Method Bias

All scale items of the current questionnaire were answered used self-reported method where same sample respondent was asked to answer both independent and dependent factors items (Bhattacherjee, 2012; Podsakoff et al., 2003). This, in turn, creates a concern of common method bias. Therefore, 25 unremoved research questions for the eight constructs (PRS; PVD; PVN; SE; PVR; RC; STA; and CIN) were all subjected to Harman's single-factor (Harman, 1976; Podsakoff et al., 2003). The yielded results of Harman's single-factor clearly assured that no single factor emerging and 41. 357 per cent of variance was accounted in the first factor which is than the threshold value (50 per cent) as recommended by Podsakoff et al., (2003). Therefore, there is no concern of common method bias in the current study data.

5.3 Descriptive Statistics of the Measurement Items

Table 3 shows that the current study participants positively value scale items used to measure personalization as the average mean for these items was about 5.90 with standard deviation value 1.16. Three items used to reflect perceived value of information disclosure were also largely rated by participants as the average mean value for these items was about 6.50 with standard deviation value 1.16. Likewise, four items of self-efficacy were positively valued with average mean value 5.64 and standard deviation value of 1.13. Three items used to measure structural assurance were able to capture an average mean value 6.16 and standard deviation value of 1.27. On the other hand, privacy invasion items were rated with lower average mean value (3.39). Similar to privacy invasion, perceived severity items and response cost items were negatively rated by the current study participants with average mean values 3.01 and 3.22 respectively. Finally, the current study participants seem to be motivated to continue using contactless payment as the average mean value of the scale items used to measure continued intention was about 6.16 and standard deviation value 1.10.

Table 3: Descriptive Statistics of the Measurement Items

Contract	Item	Mean	Standard Deviation
Personalization	PRS1	6.11	1.18
	PRS2	6.08	1.25
	PRS3	6.14	1.09
	PRS4	5.94	1.16
	Average	5.90	1.17
Perceived value of information disclosure	PVD1	6.08	1.13
	PVD2	5.94	1.21
	PVD3	6.14	1.13
	Average	6.50	1.15
Privacy Invasion	PVN1	3.34	1.39
	PVN2	3.49	1.34
	PVN3	3.35	1.46
	PVN4	3.39	1.41
	Average	3.39	1.40
Self-efficacy	SE1	5.78	1.12
	SE2	5.64	1.15
	SE3	5.61	1.08
	SE4	5.53	1.18
	Average	5.64	1.13
Response cost	RC1	3.12	1.17
	RC2	3.28	1.16
	RC3	3.26	1.16
	RC4	3.22	1.20
	Average	3.22	1.17
Perceived severity	PVR1	3.02	1.24
	PVR2	3.08	1.27
	PVR3	2.92	1.29
	PVR4	3.05	1.22
	Average	3.01	1.25
Structural assurance	STA1	6.17	1.31
	STA2	6.10	1.29
	STA3	6.21	1.23
	Average	6.16	1.27
Continued intention	CIN 1	6.14	1.14
	CIN 2	6.18	1.11
	CIN 3	6.16	1.07
	Average	6.16	1.10

5.4 Structural Equation Modelling Analysis

5.4.1 Measurement Model

Eight latent constructs and twenty nine scale items were targeted in the first stage of the structural Equation Modelling Analysis: measurement model analyses. A number of fit indices (i.e. CMIN/DF; GFI; AGFI; NFI; CFI; RMSEA) were considered to evaluate model goodness of fit. Yet, the first version of the measurement model was able to adequately fit the observed data as the number of fit indices (GFI= 0.877; AGFI = 0.784; NFI = 0.886; CFI = 0.891) did not exist within their recommended level (Anderson and Gerbing, 1988; Byrne, 2010; Bagozzi and Yi, 1988). The measurement model was, therefore, revised by removing

scale items that have factor loading value less than 0.50 (Byrne, 2010; Hair et al., 2006). By inspecting the standardised regression weight table, PRS1; SE1; SE4; and PVR4 were noticed to have a factor loading value less than 0.50, and therefore, all of these items were removed from the measurement model. Then, the revised version of the measurement model was tested with 25 scale items and all fit indices were found within their recommended level as such CMIN/DF was 1.955, GFI= 0.908, AGFI= 0.822, NFI= 0.927, CFI= 0.930 and RMSEA= 0.062 (see Table 3).

Table 4: Results of Measurement Model

Fit indices	Cut-off point	Initial measurement model	Modified measurement model
CMIN/DF	≤3.000	2.011	1.955
GFI	≥ 0.90	0.877	0.908
AGFI	≥ 0.80	0.784	0.822
NFI	≥ 0.90	0.886	0.927
CFI	≥ 0.90	0.891	0.930
RMSEA	≤ 0.08	0.068	0.062

CMIN/DF: Chi-Square value (χ^2)/Degree of freedom
GFI: Goodness of Fit Index
AGFI: Adjusted Goodness of Fit Index
NFI: Normed Fit Index
CFI: Comparative Fit Index
RMSEA: Root Mean Square Error of Approximation

5.4.2 Construct Reliability and Validity

As seen in Table 5, all constructs were able to match the main requirements pertaining to constructs validity and reliability (Anderson and Gerbing, 1988; Hair et al., 2010; Nunnally, 1978). For example, composite reliability (CR) values for eight constructs were noticed to be above 0.70 as suggested by Fornell and Larcker (1981) and Hair et al. (2010). The highest CR value (0.905) was recorded for CIN while the lowest CR value was observed for PRS (0.814). Cronbach's coefficient alpha was also tested for all constructs and was found to be above 0.70 as recommended by Nunnally (1978). CIN (0.904) was able to account the largest coefficient alpha value while PRS (0.811) accounted the lowest value in this respect.

Table 5: Constructs Reliability and Validity

	CR	Cronbach's alpha (α)	AVE
PVN	0.854	0.852	0.596
PRS	0.814	0.811	0.594
PVD	0.848	0.843	0.650
CIN	0.905	0.904	0.704
PVR	0.773	0.772	0.533
SE	0.869	0.867	0.770
STA	0.900	0.898	0.750
RC	0.888	0.884	0.615

PVN: Privacy Invasion
PRS: perceived personalization
PVD: Perceived value of information disclosure
CIN: Continued intention
PVR: Perceived severity
SE: Self-efficacy
STA: Structural assurance
RC: Response cost

Average variance extracted (AVE) values for eight latent constructs were found to be above 0.50 as well (Fornell and Larcker, 1981; Hair et al, 2010). The maximum value of AVE (0.770) was for SE where the lowest value of AVE was PVR (0.533). Further, the unremoved scale items captured a standardized regression weight value higher than 0.50 as seen in Table 7 (Hair et al., 2010). This, in turn, supports the convergent validity of the scale items used in the current study. Furthermore, the inter-correlation values between latent constructs were less than the squared root of AVE calculated for each constructs (see Table 6). Accordingly, criteria related to discriminant validity were matched in the current study constructs and scale (Fornell and Larcker, 1981).

Table 6: Discriminant Validity

	PVN	PRS	PVD	CIN	PVR	SE	STA	RC
PVN	**0.772**							
PRS	0.197	**0.771**						
PVD	0.229	0.399	**0.806**					
CIN	0.053	0.375	0.622	**0.839**				
PVR	0.430	0.417	0.487	0.503	**0.730**			
SE	0.215	0.458	0.448	0.521	0.593	**0.877**		
STA	0.176	0.581	0.623	0.575	0.543	0.521	**0.866**	
RC	0.427	0.419	0.607	0.453	0.446	0.414	0.584	**0.784**

PVN: Privacy Invasion
PRS: perceived personalization
PVD: Perceived value of information disclosure
CIN: Continued intention
PVR: Perceived severity
SE: Self-efficacy
STA: Structural assurance
RC: Response cost

Table 7: Standardized Regression Weights

			Estimate
PRS2	<---	PRS	.789
PRS3	<---	PRS	.712
PRS4	<---	PRS	.808
PVD1	<---	PVD	.764
PVD2	<---	PVD	.848
PVD3	<---	PVD	.805
PVN1	<---	PVN	.638
PVN2	<---	PVN	.858
PVN3	<---	PVN	.736
PVN4	<---	PVN	.837
SE2	<---	SE	.781
SE3	<---	SE	.964
PVR1	<---	PVR	.695
PVR2	<---	PVR	.794
PVR3	<---	PVR	.696
RC1	<---	RC	.755
RC2	<---	RC	.802
RC3	<---	RC	.856
RC4	<---	RC	.712
STA1	<---	STA	.886
STA2	<---	STA	.874
STA3	<---	STA	.838
CIN1	<---	CIN	.817
CIN2	<---	CIN	.839
CIN3	<---	CIN	.862

PVN: Privacy Invasion
PRS: perceived personalization
PVD: Perceived value of information disclosure
CIN: Continued intention
PVR: Perceived severity
SE: Self-efficacy
STA: Structural assurance
RC: Response cost

5.4.4 Structural Model Analyses

At the second stage of the SEM analyses, structural model, the predictive validity of the conceptual model and research hypotheses were tested. All fit indices of the structural model were noticed to be within their threshold level as such CMIN/DF was 1.972, GFI= 0.902, AGFI= 0.815, NFI= 0.922, CFI= 0.928 and RMSEA= 0.067. The proposed model was able to predict about 62%, 57%, and 46% of variance in PVN, CIN and PVD respectively. According to path coefficient analyses, PRS significantly impact PVD (γ=0.523, p<0.000). A significant and negative relationship was also approved between PVN and PVD (γ=-0.232, p<0.005). Structural assurance was able to significantly hinder PVN (γ=-0.156, p<0.022). Strong and positive causal associations were confirmed between both PVR (γ=0.368, p<0.000) and RC (γ=0.343, p<0.000) with PVN. Yet, self-efficacy did predict any variance in

PVN (γ=-0.060, p<0.381). Finally, both PVD (γ=0.523, p<0.000) and PVN significantly predict CIN.

Table 8: Hypotheses Testing

H#	Hypothesized path			Estimate	S.E.	C.R.	P-Value	Empirical evidence
H1	PVD	<---	PRS	.523	.112	4.684	***	Supported
H2	CIN	<---	PVD	.356	.077	4.617	***	Supported
H3	PVD	<---	PVN	-.232	.083	-2.779	.005	Supported
H4	CIN	<---	PVN	-.262	.084	-3.116	.002	Supported
H5	PVN	<---	SE	-.060	.069	-.876	.381	N.S
H6	PVN	<---	RC	.343	.077	4.441	***	Supported
H7	PVN	<---	PVR	.368	.096	3.831	***	Supported
H8	PVN	<---	STA	-.156	.068	-2.287	.022	Supported

PVN: Privacy Invasion
PRS: perceived personalization
PVD: Perceived value of information disclosure
CIN: Continued intention
PVR: Perceived severity
SE: Self-efficacy
STA: Structural assurance
RC: Response cost

6. Discussion

As argued in the introduction section, personalization–privacy paradox in Fintech (i.e. contactless payment) has been considered as a gap which requires further exploration and examinations (Karwatzki et al., 2017; Lei et al., 2022). Therefore, this study empirically examined the impact of such paradox on the customer's continued intention to keep using contactless payment. So as to provide a full picture regarding the factors shaping the customers' perception and intention toward contactless payment, protection motivation theory was also integrated in the current study model. Based on data collected from 297 of actual users of contactless payment, it has been empirically supported what has been proposed in the conceptual model. For example, the proposed model was able to adequately fit the observed data as all fit indices were noticed to be within their recommended level (i.e. CMIN/DF=1.972, GFI= 0.902, AGFI= 0.815, NFI= 0.922, CFI= 0.928 and RMSEA= 0.067). The predictive validity of the current propose model was also supported as the R^2 values accounted in the PVD (46%); PVN (62%); and CIN (57%) were adequately high. This, in turn, supports selection personalization–privacy paradox and protection motivation theory as theoretical foundation for the current proposed model.

According to path coefficient analyses (see Table 8), most of the research hypotheses were supported to be significant. The strongest causal relationship was noticed between PRS and PVD **(*H1*)**. This means that contactless payment users, who have experienced and enjoyed

with a high level of personalized services, positively value of information disclosure. Customers are mature enough to realize that a high level of personalization cannot be achieved without disclosing a large portion of their information (Lee and Rha, 2016; Lei et al., 2022; Pal et al., 2020). Such results are in the line with what has been previously confirmed by Xu et al. (2011) and Pal et al. (2020) regarding the impact of personalization on the perceived value of information disclosure.

On the other hand, privacy invasion significantly hinders the perceived value of information disclosure **(*H3*)**. To put it differently, customers, who have a high level of fears of invasion privacy, are more likely to underestimate the value of information disclosure regardless the level of personalization they could have. It is also important to indicate that issues related to privacy invasion and concerns seem to be more critical and sensitive from the customer's perspective over the financial sitting (Alalwan et al., 2017; Alalwan et al., 2018). Over the prior literature, there are a number of studies (i.e. Buhalis and Foerste, 2015; Lee and Rha, 2016; Lei et al., 2022; Xu et al., 2011) that have approved the negative influence of privacy invasion on the customer' reaction and perception toward new systems.

The yielded results of path coefficient analyses supported the impact of three predictors of privacy invasion; namely, response cost **(*H6*)**, perceived severity **(*H7*)**, and structural assurance **(*H8*)**. In details, perceived severity was the strongest increasing consumer tension and fears pertaining to privacy invasion. As argued in the conceptual model, the negative outcome arising from invasion of the personal and financial information of the customer are not limited to the financial loss only, but there are psychological effects that negatively affect the consumer experience and perception of the value of high-tech financial services (i.e. contactless payment). The current study results regarding the crucial impact of perceived severity are similar to these reported by other studies such as Gaube et al. (2019); Pal et al. (2020); and Boehmer et al. (2015).

Response cost is also approved to play a significant role in maximizing the customers' concerns and fears of privacy invasion. According to the current study results, a high level of privacy invasion was noticed among the consumer who expects high costs of time and effort to deal with any penetration of their financial and personal information as a result of using contactless payment. This is in the line with what has been suggested by Protection Motivation Theory regarding the role of response cost as one of the main dimensions that

determine the technology user's ability to cope with any risk or invasion privacy (Vance et al., 2012; Scarpa and Thiene, 2011; Al-Sharafi et al., 2021).

Conversely, structural assurance was empirically confirmed to play a significant role in hindering privacy invasion. Such results implies that customers' concerns about privacy invasion are more likely to be very low level and less influential in the case that consumer is aware of the existence of solid legal and technical framework and that guarantees the secure use of technology and prevents hacking or misuse of customers' personal information (Zhou, 2012; Park et al., 2015). Over the prior IS and FinTech literature, there are several examples about the studies that have proven the significant role of structural assurance (i.e. Wingreen et al., 2019; Geebren et al., 2021; Thusi et al., 2020; Sarkar et al., 2020).

The yielded results of path coefficient analyses supported the significant impact of PVD on the CIN **(*H2*)** with regression weight value of 0.356. Such results illustrates that customers, who perceive information disclosure useful and beneficial, are more motivated to keep using contactless payment methods. In different words, if customers highly value the benefits and benefits of disclosure of information compared to associated risks, they are more likely to positively value information disclosure, and accordingly, being more inclined to use contactless payment in future. The significant impact of PVD has been commonly reported by different studies over the related area of Fintech (i.e. Xu et al., 2011; Pal et al., 2011; Lin et al., 2021; Nikkhah et al., 2021).

As expected, a strong and negative causal relationship was confirmed between PVN and CIN **(*H4*)**. This means that customers, who expect that the use of electronic payment may expose their privacy and financial information at risk, will be less interested in using such technology in the future. Such results would be returned to the fact that having a high level of personal experience with contactless payment applications requires disclosing more personal information of the consumer, and thus becomes more vulnerable to being hacked and violating his privacy (Bolderdijk et al., 2013; Lee and Cranage, 2011; Xu et al., 2011). The negative impact of invasion privacy has been empirically approved in different sectors such as tourism (Buhalis and Foerste, 2015; Lee and Rha, 2016; Lei et al., 2022); travel Web sites (Lee and Cranage, 2011); location based services (Xu et al., 2011).

6.1 Theoretical contribution

This study has theoretically contributed to the current area of Fintech and contactless payment in particular in different aspects. Firstly, this study has integrated both

personalization–privacy paradox and protection motivation theory in one model. Accordingly, the current study has a value by providing new and full picture about new kinds of inhibitors and enablers of customers' continued intention to keep using contactless payment. This study also helps both researchers and practitioners to discover new mechanisms that could shape customer' behaviour and perception toward contactless payment. Furthermore, this study has proposed perceived value of information disclosure as a consequence of both personalization and privacy invasion. Accordingly, further understanding has been added about the way that customers cognitively compare between the pros (i.e. high level of personalized experience) and cons (i.e. privacy invasion) of using contactless payment.

Secondly, Personalization–privacy paradox has not been fully examined over the related area of Fintech and contactless payment in general. Therefore, this study was able to extend the theoretical horizon Personalization–privacy paradox to new area (i.e. contactless payment) and new cultural context (Saudi Arabia). Further, this study was able to empirically approve the applicability of Personalization–privacy paradox over the context of contactless payment. By doing so, this study has enriched the current understanding of the dilemma between a customer's desire for a more personalized experience and their privacy and security concerns.

Thirdly, this study was not limited to research only personalization–privacy paradox but also looking at new factors that would specially predict the customers' perception of privacy invasion. For example, this study has empirically approved the significant influence of both response cost and perceived severity. Thus, this study was able to provide a more accurate picture of the expected negative consequences of the invasion of personal and financial information of the customer, and that these consequences are not limited to the costs of time and effort, but there are also psychological consequences that negatively affect the consumer experience with contactless payment methods. Another theoretical contribution was captured in the current study by proposing and empirically supporting the role of structural assurance. This, in turn, provides further understanding regarding the most important mechanisms that help mitigate the impact of consumer concerns regarding privacy invasion.

6.2 Practical implications

The value of this study is not limited only to the theoretical framework, but extends to the practical side by providing a set of practical recommendations that help marketers and designers of contactless payment. Indeed, results of the current study assure the importance

of discovering customers' perception and attitudes toward such dilemma (personalization and privacy paradox). Therefore, it is highly suggested polling the customers opinions and discovering if they prefer to have high level of personalization or protecting their own privacy (Lee and Rha, 2016). This would help designers to discover which aspects that have to be considered more privacy protection or personalized experience. In this respect, it is also important assured customers that protecting customer privacy is not contradict with high level of personalization. This would be attained through a high degree of transparency with the consumers regarding the information collected and for what purposes it is used. In this regard, the consumers must also be made aware that the benefit of collecting this information is for the consumers themselves by providing services at a level that matches their expectations and personal preferences. Customers should be empowered to have a full freedom and control in identifying which kind of personal information should be disclosed (Pal et al., 2020).

The positive impact of PVD gives marketers clues about the importance of conducting promotional campaigns that increase consumer awareness of the value and benefits of using PVD. So as to reach a wide range of customers segments, such campaigns would be delivered to the customers' side using offline or online platforms (i.e. social media; location based advertising; YouTube) (Dwivedi et al., 2018).

Results of the current study also give clues regarding the importance of structural assurance in alleviating customers' concerns of privacy invasion. In this respect, service providers should pay more attention to the technical features (i.e. encryption and authentication) that guarantee a secure and safe using of contactless payment. A high level of collaboration between service providers of contactless payment with official and legal authorities is very important so as to build and sustain a legal framework protecting customer from any misuse of their personal information. Another kind of collaboration with internet service providers and other stakeholders (Visa; MasterCard; Apple; and Samsung) are really critical to assure a high level of privacy and security as well.

To address the challenges associated with the cost of response, a high level of security must be provided in the use of contactless payment methods for free without any expenses. Additionally, In the event of a problem with the customer, his/her information or account being hacked, it must work to solve these problems without incurring any additional costs or burdens to the customer. Further, more efforts should be spent to make the policy of

compliance with the security of contactless payment easy and does not require financial costs, time or efforts. As for perceived severity, service providers should approve their capabilities in controlling security incidents or threats. In this respect, it is highly recommended to publish firms' safety protocols on their authorized websites (Leung and Cai, 2021). Such of these published information should also contain a clear and precise framework for all procedures to be followed by customers to guarantee a secured use of contactless payment, and accordingly, avoiding the negative outcome arising from invasion of the personal and financial information of the customer.

6.3 Limitations and future research directions

Even though this study has comprised a theoretical and practical contribution to the area of contactless payment as reported above, there are a number of limitations which would be considered and addressed in future. The current study model was proposed based on two models (i.e. Personalization–privacy paradox and protection motivation theory). Yet, these models do not cover other important factors (i.e. technology interactivity; technology readiness; social influence; trust; prior experience; etc.). Therefore, future studies would pay more attention regarding the impact of these factors so as to have a full picture about the customer's behaviour and perception toward contactless payment.

This study has look at the direct impact of perceived value of information disclosure on the continued intention. Therefore, it would be useful for future studies to look at the direct and indirect impact (mediating role) of PVD on the relationship between customer' intention and factors such as perceived personalization; privacy invasion; and protection motivation theory factors. This study has only focused on the customers' continued intention while there are other aspects (i.e. customer attitudes; customers' satisfaction; customers' usage experience; brand image; brand engagement) have not been proposed in the current study model, and therefore, present worth directions to be considered by future studies. The current study data was collected using a convenience sample of actual users of contactless payment methods. Therefore, there is a concern regarding the generalizability of the current study results to other kind of customers who have not used contactless payment. Future studies are highly suggested to consider non-users perspective or even positional users with disability to see how they would react toward issues of Personalization–privacy paradox that related to contactless payment usage. Furthermore, this study has employed cross-sectional data, which poses limitations in terms of drawing a firm conclusion. To overcome this limitation, as recommended by Maier et al. (2023), future studies extending this work should employ either

a configurational approach or integrate cross-sectional data into mixed- or multi-method designs. Finally, Generative AI applications (for example, ChatGPT3, ChatGPT4, BARD) are emerging technologies that would likely play an important role in the Fintech ecosystem. Hence, future studies should examine the adoption, usage, and impact of Generative AIs (such as ChatGPT) in relation to financial services marketing, provision, and requisition (Dwivedi et al., 2023).

7. Conclusion

Personalization–privacy paradox in Fintech (i.e. Contactless payment) has been rarely examined, and accordingly, it was considered as a gap to be covered in the current study (Karwatzki et al., 2017; Lei et al., 2022). In addition to Personalization–privacy paradox, protection motivation theory was also formulated in the current study model so as to provide a comprehensive picture regarding the main factors that could either hinder or contribute to the customer continued intention to use of FinTech (i.e. Contactless payment). In details, personalization was proposed as key factor contributing perceived value of information disclosure while privacy invasion was theorised as hinder of perceived value of information disclosure. According to protection motivation theory, perceived severity; response cost; self-efficacy; and perceived structural assurance were proposed as key factors predicting privacy Invasion (Vance et al., 2012; Williams et al., 2015; Li, 2012; Ifinedo, 2012). The empirical part of the current study was conducted in Saudi Arabia by collecting the primary data using online questionnaire from a convenience sample of the actual users of contactless payment. Based on SEM analyses, both personalization and privacy invasion were supported to have a significant impact on perceived value of information disclosure, which in turn, impact continued intention to use contactless payment. Perceived severity; response cost; and perceived structural assurance were also confirmed to have a significant influence on privacy invasion. Yet, self-efficacy does not have any influence on privacy invasion

References

Aguirre, E., Mahr, D., Grewal, D., De Ruyter, K., and Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing*, 91(1), 34–49.

Aharony, N. (2016). Relationships among attachment theory, social capital perspective, personality characteristics, and Facebook self-disclosure. *Aslib Journal of Information Management*, 68(3), 362-386.

Aladwani, A. M., & Dwivedi, Y. K. (2018). Towards a theory of SocioCitizenry: Quality anticipation, trust configuration, and approved adaptation of governmental social media. *International Journal of Information Management*, 43, 261-272.

Alalwan, A. A., Algharabat, R. S., Baabdullah, A. M., Rana, N. P., Qasem, Z., and Dwivedi, Y. K. (2020). Examining the impact of mobile interactivity on customer engagement in the context of mobile shopping. *Journal of Enterprise Information Management*, 33(3), 627-653.

Alalwan, A. A., Dwivedi, Y. K., and Rana, N. P. (2017). Factors influencing adoption of mobile banking by Jordanian bank customers: Extending UTAUT2 with trust. *International Journal of Information Management*, *37*(3), 99-110.

Alalwan, A. A., Dwivedi, Y. K., Rana, N. P., and Algharabat, R. (2018). Examining factors influencing Jordanian customers' intentions and adoption of internet banking: Extending UTAUT2 with risk. *Journal of Retailing and Consumer Services*, *40*, 125-138.

Al-Emran, M., Granić, A., Al-Sharafi, M. A., Ameen, N., and Sarrab, M. (2020). Examining the roles of students' beliefs and security concerns for using smartwatches in higher education. *Journal of Enterprise Information Management*, 34(4), 1229-1251.

Al-Okaily, M., Alalwan, A.A., Al-Fraihat, D., Rehman, S. U., and Alkhwaldi, A.F. & Al-Okaily, A., (2022). Investigating Antecedents of Mobile Payment Systems Decision Making: A Mediated Model. *Global Knowledge, Memory and Communication*. Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/GKMC-10-2021-0171.

Al-Qudah, A. A., Al-Okaily, M., Alqudah, A. & Ghazlat, A. (2022). Mobile payment adoption in the time of the COVID-19 pandemic. *Electronic Commerce Research*,. https://doi.org/10.1007/s10660-022-09577-1.

Al-Sharafi, M. A., Al-Qaysi, N., Iahad, N. A., and Al-Emran, M. (2021). Evaluating the sustainable use of mobile payment contactless technologies within and beyond the COVID-19 pandemic using a hybrid SEM-ANN approach. *International Journal of Bank Marketing*, 40(5),1071-1095.

Anderson, J. C. and Gerbing, D. W. (1988). Structural equation modelling in practice: A review and recommended two-step approach. Psychological Bulletin, 103(3), 411-423.

Baabdullah, A. M., Alalwan, A. A., Rana, N. P., Patil, P., & Dwivedi, Y. K. (2019). An integrated model for m-banking adoption in Saudi Arabia. *International Journal of Bank Marketing*, 37(2), 452-478

Bagozzi, R. P. and Yi, Y. (1988). On the evaluation of structural equation models. Journal of the Academy of Marketing Science, 16(1), 74-94.

Banerjee, S., and Sreejesh, S. (2021). Examining the role of customers' intrinsic motivation on continued usage of mobile banking: a relational approach. *International Journal of Bank Marketing*, 40(1), 87-109.

Bhattacherjee, A. (2012). *Social science research: Principles, methods, and practices*. (2nd Ed.). Florida, USA: AnolBhattacherjee.

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., and Cotten, S. (2015). Determinants of online safety behaviour: Towards an intervention strategy for college students. *Behaviour and Information Technology*, *34*(10), 1022-1035.

Bolderdijk, J., Steg, L., and Postmes, T. (2013). Fostering support for work floor energy conservation policies: Accounting for privacy concerns. *Journal of Organizational Behavior,* 34(2), 195–210.

Bounie, D., and Camara, Y. (2020). Card-sales response to merchant contactless payment acceptance. Journal of Banking and Finance, 119, 105938.

Bryman, A. (2004). *Social research methods*. Oxford: Oxford University Press.

Buhalis, D., and Foerste, M. (2015). SoCoMo marketing for travel and tourism: empowering co-creation of value. *Journal of destination marketing and management*, *4*(3), 151-161.

Byrne, B. (2010). Structural equation modeling with AMOS: Basic concepts, applications and programming. (6th Ed.). New York, USA: Taylor and Francis Group.

Cameron, J. J., Holmes, J. G., & Vorauer, J. D. (2009). When self-disclosure goes awry: Negative consequences of revealing personal failures for lower self-esteem individuals. *Journal of Experimental Social Psychology*, *45*(1), 217-222.

Chen, H. T., and Chen, W. (2015). Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 13-19.

Chen, S. J., Tran, K. T., Xia, Z. R., Waseem, D., Zhang, J. A., & Potdar, B. (2023). The double-edged effects of data privacy practices on customer responses. *International Journal of Information Management*, *69*, 102600.

Choi, B. C., Jiang, Z., Xiao, B., & Kim, S. S. (2015). Embarrassing exposures in online social networks: An integrated perspective of privacy invasion and relationship bonding. *Information Systems Research*, *26*(4), 675-694.

Cloarec, J., Meyer-Waarden, L., and Munzel, A. (2022). The personalization–privacy paradox at the nexus of social exchange and construal level theories. *Psychology and Marketing*, *39*(3), 647-661.

Cocosila, M., and Trabelsi, H. (2016). An integrated value-risk investigation of contactless mobile payments adoption. *Electronic Commerce Research and Applications*, *20*, 159-170.

Daragmeh, A., Lentner, C., and Sági, J. (2021). FinTech payments in the era of COVID-19: Factors influencing behavioral intentions of "Generation X" in Hungary to use mobile payment. *Journal of Behavioral and Experimental Finance*, *32*, 100574.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of computer-mediated communication*, *15*(1), 83-108.

Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E. L., Jeyaraj, A., Kar, A. K., ... & Wright, R. (2023). "So what if ChatGPT wrote it?" Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management*, 71, 102642.

Dwivedi, Y. K., Kelly, G., Janssen, M., Rana, N. P., Slade, E. L., & Clement, M. (2018). Social Media: The good, the bad, and the ugly. *Information Systems Frontiers*, *20*(3), 419-423.

eMarketer. (2021). Proximity mobile pay is on the rise worldwide. Available at: https://www.insiderintelligence.com/content/proximity-mobile-pay-on-rise-worldwide. Accessed on 28/5/2022.

Faqih, K. M. (2013). Exploring the influence of perceived risk and internet self-efficacy on consumer online shopping intentions: Perspective of technology acceptance model. *International Management Review*, *9*(1), 67-77.

Fornell, C. and Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18(1), 39-50.

Geebren, A., Jabbar, A., and Luo, M. (2021). Examining the role of consumer satisfaction within mobile eco-systems: Evidence from mobile banking services. *Computers in Human Behavior*, *114*, 106584.

Gomber, P., Koch, J. A., and Siering, M. (2017). Digital Finance and FinTech: current research and future research directions. Journal of Business Economics, 87(5), 537-580.

Gupta, B. B., and Narayan, S. (2021). A key-based mutual authentication framework for mobile contactless payment system using authentication server. *Journal of Organizational and End User Computing (JOEUC)*, *33*(2), 1-16.

Hair Jr., J. F., Black, W. C., Babin, B. J., and Anderson, R. E. (2010). Multivariate data analysis: A global perspective. (7th Ed.). Pearson Education International.

Hair Jr., J. F., Black, W., Babin, B., Anderson, R. E., and Tatham, R. (2006). Multivariate data analysis. (6th Ed.). New Jersey: Prentice Hall.

Harman, H. H. (1976). *Modern factor analysis*. (3rd Ed.). Chicago, IL: University of Chicago Press.

Hughes, D. L., Dwivedi, Y. K., Rana, N. P., & Simintiras, A. C. (2016). Information systems project failure–analysis of causal links using interpretive structural modelling. *Production Planning & Control*, *27*(16), 1313-1333.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security*, *31*(1), 83-95.

Kalia, P., Dwivedi, Y. K., & Acevedo-Duque, Á. (2022). Cellulographics©: A novel smartphone user classification metrics. *Journal of Innovation & Knowledge*, *7*(2), 100179.

Kamboj, S., Sharma, M., and Sarmah, B. (2021). Impact of mobile banking failure on bank customers' usage behaviour: the mediating role of user satisfaction. *International Journal of Bank Marketing*, 40(1), 128-153.

Karjaluoto, H., Shaikh, A. A., Leppäniemi, M., and Luomala, R. (2019). Examining consumers' usage intention of contactless payment systems. *International Journal of Bank Marketing*.

Karwatzki, S., Dytynko, O., Trenz, M., and Veit, D. (2017). Beyond the personalization–privacy paradox: Privacy valuation, transparency features, and service personalization. *Journal of Management Information Systems*, *34*(2), 369-400.

Kumar, P., Sharma, S. K., & Dutot, V. (2023). Artificial intelligence (AI)-enabled CRM capability in healthcare: The impact on service innovation. *International Journal of Information Management*, *69*, 102598.

Lee, C. H., and Cranage, D. A. (2011). Personalisation–privacy paradox: The effects of personalisation and privacy assurance on customer responses to travel Web sites. *Tourism Management*, *32*(5), 987-994.

Lee, C. T., & Pan, L. Y. (2022). Smile to pay: predicting continuous usage intention toward contactless payment services in the post-COVID-19 era. *International Journal of Bank Marketing*, (ahead-of-print).

Lee, J. M., and Rha, J. Y. (2016). Personalization–privacy paradox and consumer conflict with the use of location-based mobile commerce. *Computers in Human Behavior*, *63*, 453-462.

Lee, J., Kim, C., & Lee, K. C. (2022). Exploring the personalization-intrusiveness-intention framework to evaluate the effects of personalization in social media. *International Journal of Information Management*, *66*, 102532.

Lei, S. S. I., Chan, I. C. C., Tang, J., and Ye, S. (2022). Will tourists take mobile travel advice? Examining the personalization-privacy paradox. *Journal of Hospitality and Tourism Management*, *50*, 288-297.

Leung and Cai, I., Radulović, B., and Lacmanović, D. (2010, May). Contactless payment systems based on RFID technology. In *The 33rd International Convention MIPRO* (pp. 1114-1119). IEEE.

Leung, X. Y., and Cai, R. (2021). How pandemic severity moderates digital food ordering risks during COVID-19: An application of prospect theory and risk perception framework. *Journal of Hospitality and Tourism Management*, *47*, 497-505.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision support systems*, *54*(1), 471-481.

Lin, M. Y. C., Do, B. R., Nguyen, T. T., and Cheng, J. M. S. (2021). Effects of personal innovativeness and perceived value of disclosure on privacy concerns in proximity marketing: self-control as a moderator. *Journal of Research in Interactive Marketing*.

Maier, C., Thatcher, J. B., Grover, V., & Dwivedi, Y. K. (2023). Cross-sectional research: A critical perspective, use cases, and recommendations for IS research. *International Journal of Information Management*, 102625.

Marriott, H. R., Williams, M. D., & Dwivedi, Y. K. (2017). What do we know about consumer m-shopping behaviour?. *International Journal of Retail & Distribution Management, 45(6), 568-586.*

Mention, A. L. (2019). The future of fintech. *Research-Technology Management*, 62(4), 59-63.

Moghavvemi, S., Mei, T. X., Phoong, S. W., and Phoong, S. Y. (2021). Drivers and barriers of mobile payment adoption: Malaysian merchants' perspective. *Journal of Retailing and Consumer Services*, 59, 102364.

Mohamed, N., and Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, *28*(6), 2366-2375.

Nikkhah, H. R., Sabherwal, R., and Sarabadani, J. (2021). Mobile cloud computing apps and information disclosure: the moderating roles of dispositional and behaviour-based traits. *Behaviour and Information Technology*, 1-17.

Nilsson, H. (2021). Trust issues? The need to secure contactless biometric payment cards. Biometric Technology Today, 2021(1), 5-8.

Nunnally, J. C. (1978). Psychometric theory. New York, NY: McGraw-Hill.

Otterbring, T., and Bhatnagar, R. (2022). Touch, threats, and transactions: Pandemic influences on consumer responses and the mediating role of touch likelihood when shopping for fruits and vegetables. *Food Quality and Preference*, *97*, 104461.

Pal, D., Vanijja, V., and Papasratorn, B. (2015). An empirical analysis towards the adoption of NFC mobile payment system by the end user. Procedia Computer Science, 69, 13-25.

Park, M. J., Choi, H., Kim, S. K., and Rho, J. J. (2015). Trust in government's social media service and citizen's patronage behavior. *Telematics and Informatics*, *32*(4), 629-641.

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

Sandhu, R. K., Vasconcelos-Gomes, J., Thomas, M. A., & Oliveira, T. (2023). Unfolding the popularity of video conferencing apps–A privacy calculus perspective. *International Journal of Information Management*, *68*, 102569.

Sarkar, S., Chauhan, S., and Khare, A. (2020). A meta-analysis of antecedents and consequences of trust in mobile commerce. *International Journal of Information Management*, *50*, 286-301.

Scarpa, R., and Thiene, M. (2011). Organic food choices and Protection Motivation Theory: Addressing the psychological sources of heterogeneity. *Food quality and preference*, *22*(6), 532-541.

See-To, E. W., and Ngai, E. W. (2019). An empirical study of payment technologies, the psychology of consumption, and spending behavior in a retailing context. *Information and Management*, *56*(3), 329-342.

Semerikova, E. (2020). What hinders the usage of smartphone payments in Russia? Perception of technological and security barriers. *Technological Forecasting and Social Change*, *161*, 120312.

Shaw, N., Eschenbrenner, B., and Brand, B. M. (2022). Towards a Mobile App Diffusion of Innovations model: A multinational study of mobile wallet adoption. *Journal of Retailing and Consumer Services*, *64*, 102768.

Shishah, W., and Alhelaly, S. (2021). User experience of utilising contactless payment technology in Saudi Arabia during the COVID-19 pandemic. *Journal of Decision Systems*, *30*(2-3), 282-299.

Sutanto, J., Palme, E., Tan, C.-H., and Phang, C. W. (2013). Addressing the personalization–privacy paradox: An empirical assessment from a field experiment on smartphone users. *MIS Quarterly*, 37(4), 1141–1164.

Thakor, A. V. (2020). Fintech and banking: What do we know?. Journal of Financial Intermediation, 41, 100833.

Thusi, P., and Maduku, D. K. (2020). South African millennials' acceptance and use of retail mobile banking apps: An integrated perspective. *Computers in Human Behavior*, *111*, 106405.

Trütsch, T. (2020). The impact of contactless payment on cash usage at an early stage of diffusion. Swiss Journal of Economics and Statistics, 156(1), 1-35.

Vance, A., Siponen, M., and Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information and Management*, *49*(3-4), 190-198.

Vimalkumar, M., Sharma, S. K., Singh, J. B., & Dwivedi, Y. K. (2021). 'Okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants. *Computers in Human Behavior*, *120*, 106763.

Walrave, M., Vanwesenbeeck, I., and Heirman, W. (2012). Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults. *Cyberpsychology* 6, 1–16.

Williams, L., Rasmussen, S., Kleczkowski, A., Maharaj, S., and Cairns, N. (2015). Protection motivation theory and social distancing behaviour in response to a simulated infectious disease epidemic. *Psychology, health and medicine*, *20*(7), 832-837.

Wingreen, S. C., Mazey, N. C., Baglione, S. L., and Storholm, G. R. (2019). Transfer of electronic commerce trust between physical and virtual environments: experimental effects of structural assurance and situational normality. *Electronic Commerce Research*, *19*(2), 339-371.

World FinTech Report. (2021). World FinTech Report 2021. Available at: https://fintechworldreport.com/. Accessed on 29/5/2022.

Wu, C. G., and Ho, J. C. (2021). The influences of technological characteristics and user beliefs on customers' perceptions of live chat usage in mobile banking. *International Journal of Bank Marketing*, 40(1), 68-86.

Xu, H., Luo, X. R., Carroll, J. M., and Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision support systems*, *51*(1), 42-52.

Zhong, Y., Oh, S., and Moon, H. C. (2021). Service transformation under industry 4.0: Investigating acceptance of facial recognition payment through an extended technology acceptance model. *Technology in Society*, *64*, 101515.

Zhou, T. (2012). Understanding users' initial trust in mobile banking: An elaboration likelihood perspective. *Computers in human behavior*, *28*(4), 1518-1525.

Appendix

Table 1: Studies that have tested the related issues of contactless payment

Study	Factors examined	Methodology	Contactless application considered	Context
Semerikova (2020)	Slow speed, failed biometrics recognition, dead battery, perceived security, intention.	Questionnaire survey	Contactless Mobile payment	Russia
Trütsch (2020)	Contactless payment usage and cash usage	Online surveys	Contactless credit and visa cards	USA
Bounie and Camara (2020)	Acceptance of contactless payment and merchant card sales (i.e. amount, count and amount per transaction)	Using score matching and difference-in-difference techniques on	Contactless credit card	France
See-To and Ngai (2019)	Preciseness; memory error; perceived security; transaction frequency amount; source of money; payment process; perceived convenience; transaction frequency; payment timing.	Questionnaire	Contactless smart cards	Hong Kong
Cocosila and Trabelsi (2016)	Utility value; hedonic value; social value; perceived risk; integrated value-risk, and behavioural intention	Questionnaire	Credit card contactless with smartphones	Canada
Daragmeh et al. (2021)	Perceived usefulness; perceived ease of use; subjective norm; and perceived COVID-19 risk	Online questionnaire	Contactless Mobile payment	Hungary
Al-Sharafi et al. (2021)	Expectation confirmation; perceived usefulness; perceived severity; perceived vulnerability; self-efficacy;	Online survey	Contactless Mobile payment	Malaysia

	response cost; perceived trust; satisfaction; and sustainability			
Karjaluoto et al. (2020)	Performance expectancy; effort expectancy; hedonic motivation; habit; perceived risk; brand engagement; brand community; satisfaction; behavioural intention; and actual usage behaviour	Online survey	Different methods of contactless payment systems	Finland
Shishah and Alhelaly (2021)	Emotions; cognitions; attitudes; and behaviour	Online survey	Contactless credit card	Saudi Arabia
Otterbring and Bhatnagar (2022)	Pandemic Impact ; Payment preferences; and Touch likelihood	Scenario-based online experiment	Contactless credit and mobile payment	-
Zhong et al. (2021)	Perceived usefulness; perceived enjoyment; facilitating conditions; personal innovativeness; coupon availability; attitude; gender; behavioural intention.	Online questionnaire	Facial recognition payment	China
Lee and Pan (2022)	Relative advantage; compatibility; attractiveness; perceived security; Performance expectancy; effort expectancy; emotions; and continued intention	Online survey	Facial recognition payment	China