Telematics and Informatics 77 (2023) 101939

Contents lists available at ScienceDirect

Telematics and Informatics

journal homepage: www.elsevier.com/locate/tele

Disentangling facial recognition payment service usage behavior: A trust perspective

Chenglong Li [*], Hongxiu Li

Department of Information and Knowledge Management, Tampere University, Tampere, Finland

ARTICLE INFO

Keywords:
Facial recognition payment
Continuance intention
Trust
Privacy
Security

ABSTRACT

Facial recognition payment (FRP) technology has been used as an innovative digital approach to payment services. This study develops a model to investigate how user trust—including trust in FRP service providers and FRP—affects users' continuance intentions toward FRP services. We also propose that trust in FRP itself is affected by perceived vulnerability, perceived security, and perceived response efficacy from a privacy and security perspective. Our research model was empirically tested via a partial-least-squares analysis with survey data collected from 217 FRP users in China. The results show that trust in both FRP service providers and FRP itself positively affects users' continuance intentions, and trust in service providers affects trust in FRP. Perceived security and response efficacy positively affect trust in FRP. This research contributes to the literature on FRP and trust, offering practical implications for FRP service providers on how to manage individual users' FRP-related privacy concerns while enhancing user trust in FRP, which facilitates continuous FRP use.

1. Introduction

Advancements in facial recognition technologies (FRT) have facilitated the popularity of facial recognition payment (FRP) methods in China. This innovative digital payment method enables people to authorize a payment using their face once they have connected their facial information to their online payment account or bank account (Liu et al., 2021; Zhang and Kang, 2019). FRP provides a convenient, fast, and efficient service since it can speed up payment interactions and enhance transaction efficiency (Liu et al., 2021). Three leading online payment service providers operate in the Chinese market: Alipay, which launched the FRP device Dragonfly in 2018; WeChat, which introduced a similar machine, Frog, in 2019; and China UnionPay, which released the Face Scan Pay product in 2019 (Liu et al., 2021). In 2019, FRP was reported to have been used in 1,000 convenience stores in China by 100 million registered Chinese users (Horswill, 2021), and this number was estimated to reach 760 million in 2022 (iiMedia Report, 2019).

FRP's emergence and popularity have attracted scholarly attention. For instance, Moriuchi (2021) examined the factors influencing users' intentions to use FRP in both offline and online retail settings based on the unified theory of acceptance and use of technology (UTAUT) (Venkatesh et al., 2003) and theory of mind (Premack and Woodruff, 1978), finding that use intentions in both settings are positively determined by performance expectations and social influences, while users' trust and attitudes are significant mediators. Based on the technology acceptance model, Zhong et al. (2021) found that intentions to use FRP are influenced by perceived usefulness, perceived ease of use, perceived enjoyment, facilitating conditions, coupon availability, personal innovativeness, and attitude. From a valence-based perspective, Palash et al. (2022) discovered that FRP use intentions are positively influenced by a relative

[*] Corresponding author.

https://doi.org/10.1016/j.tele.2023.101939
Received 30 August 2022; Received in revised form 8 December 2022; Accepted 9 January 2023
Available online 10 January 2023

advantage, initial trust, perceived playfulness, and the need for uniqueness, while they are negatively influenced by perceived risk and technophobia. However, these studies have focused mainly on initial FRP adoption, largely ignoring users' continuance intentions, which refer to users' intention to continue using an IS over a long period. Continuance intention has been stated as crucial for the sustainability of an IS, since an IS's eventual success depends on users' continued usage (Bhattacherjee, 2001). Retaining users can help FRP service providers increase profitability and reduce costs (Bhattacherjee, 2001; Cao et al., 2018). Therefore, which factors facilitate users' continuance intentions regarding FRP services must be investigated.

The information systems (IS) literature has demonstrated user trust's importance in facilitating continuance intentions regarding payment technologies since payment services involve monetary transactions and require a high level of security. For instance, based on trust transfer theory, Cao et al. (2018) found that the trust transfer process from online payments to mobile payments positively affects users' continuance intentions through their satisfaction with mobile payments. Shao et al. (2019), meanwhile, found that user trust in a mobile payment platform positively affects continuance intentions regarding a mobile payment service. *Trust* can be defined differently, such as faith in technology, an institution, and a human. In the FRP context, users may trust FRP technology itself and FRP service providers.

While these studies offer important insights into the role of trust in explaining continuance intention toward a payment technology, FRP has been largely ignored thus far. Compared with other payment technologies, such as credit cards, online payment, and mobile payment, a unique advantage of FRP is that it does not require any physical cards or mobile devices (Dang et al., 2022). Therefore, FRP is much more convenient than other payment technologies. On the other side, a major concern in FRP is privacy and security issues, which have been argued to be more serious than other payment technologies. Unlike passwords and Personal Identification Numbers (PINs), users' facial information is highly private biometric information, which is permanent and not editable. Once users' facial information is leaked, users cannot change their facial information on facial recognition payment systems to protect their privacy and finance security. Additionally, the facial information captured by FRP may be hacked and misused beyond FRP, such as surveillance (Leong, 2019; Yeung et al., 2020). Therefore, FRP users could worry more about their privacy and security in FRP use than in using other payment technologies. Given the differences between FRP and other payment technologies, the trust's role in motivating users' continuance intention to use FPR and the determinants of trust might differ from those in other payment technologies. Hence, further examinations are required.

Additionally, prior studies have mainly investigated trust in explaining continuance intentions regarding payment technology from either a technological view—such as by exploring trust in a mobile payment technology (e.g., Cao et al., 2018)—or an institutional view, such as examining trust in digital payment service providers (e.g., Mallat, 2007). Little research has adopted an integrated perspective on technology and institutions to examine their roles in explaining users' continuous use of digital payment methods, as well as the relationship between technology-based trust and institution-based trust—particularly in the innovative FRP context. Investigating the association between technology-based and institution-based trust may also advance the understanding of these trust types' interdependence in the FRP context.

Furthermore, though trust has been cited as an important factor determining intentions to use FRP services (Hu et al., 2021; Palash et al., 2022), few studies have examined the antecedents of trust in FRP by highlighting privacy and security concerns despite FRP's involving users' facial information, thus requiring high levels of privacy protection and security in FRP. The collection, storage, and application of users' facial information can cause concerns about potential hacks and the misuse of such intensely personal identifiers, particularly in surveillance. Therefore, privacy and security concerns are crucial in the FRP context (Zhang and Kang, 2019), and they may significantly influence user trust in this technology. Accordingly, explaining how privacy and security issues influence user trust can add valuable insights to FRP trust-building.

To fill the above-mentioned research gap, this study investigates how user trust in institutions and technology affects continuance intentions regarding FRP services, as well as what factors determine trust in FRP from the privacy and security view. Specifically, we examine how user trust in FRP service providers and FRP itself affect FRP continuance intentions. Trust in FRP is determined by factors related to privacy and security issues, including perceived vulnerability, perceived response efficacy, and perceived security. In explaining these connections, this study contributes to the literature. First, unlike prior studies that have focused on either technology-based or institution-based trust (e.g., Cao et al., 2018; Mallat, 2007), this study examines how user trust facilitates FRP continuance intentions by integrating technological and institutional perspectives (i.e., trust in FRP itself and trust in FRP service providers) and by advancing the understanding of different trust types' interdependence. Second, this study explains the antecedents of trust in FRP from a perspective based on privacy and security, which are highly relevant to the FRP context.

2. Literature review

2.1. Facial recognition payment

FRP relies on face recognition technology, which uses algorithms to capture, extract, and compare individuals' biometric facial information to verify their personal identity (Zhang and Kang, 2019). A FRP user must pre-register as a member of an FRP service and link his/her facial information to an online payment account (e.g., an Alipay or WeChat account) or bank account. When making a purchase, customers need only stand still and look squarely at the camera of an FRP device or smartphone, and then the captured facial information is compared to facial information stored in a database to validate a transaction. Once the two sets of facial information are matched, the payment is confirmed.

On the one hand, FRP offers some advantages compared to other digital payment methods, such as online payment and mobile payment (Moriuchi, 2021; Zhang and Kang, 2019). First, it is faster since the entire validation process takes only several seconds.

Table 1
Summary of studies on trust in payment technologies in the information systems (IS) field.

Reference	Trust type	Research method	Theoretical lens	Trust antecedents	Trust consequences
Cao et al., 2018	Trust in mobile payments	Survey (N = 219)	Trust transfer theory	Trust in online payment; Perceived similarity; Perceived entitativity	Satisfaction with mobile payment; Continuance intentions
Chin et al., 2022	Trust in mobile payments	Survey (N = 234)	Valence framework	Privacy; Security; Familiarity	Perceived benefits; Intention to use; Perceived risk
Franque et al., 2022	Trust in mobile payments	Survey (N = 384)	Task technology fit model; Expectation confirmation model	Benevolence; Competence; Integrity	Continuance intentions; Use
Gao and Waechter, 2017	Trust in mobile payment	Survey (N = 851)	Valence framework	Information quality; System quality; Service quality; Perceived uncertainty; Perceived asset specificity	Perceived benefits; Perceived convenience
Gong et al., 2020	Trust in mobile payment	Survey (N = 491)	Trust-based acceptance model; Trust transfer theory	Cognitive trust in web payments; Emotional trust in web payments; Perceived entitativity	Intention to use mobile payment
Hillman and Neustaedter, 2017	Trust in mobile payment services	Qualitative study (diary, N = 161; and interview, N = 21)	Trust-production mechanisms	Few trust concerns when shopping on mobile devices; Trust concerns emerged along with pre-purchase anxiety and mental model challenges in offline shopping	/
Hu et al., 2021	Trust in FRP	Survey (N = 1,200)	Perceived value; Perceived trust	Privacy risk; Financial risk; Perceived value	Use intentions
Kar, 2021	Trust in mobile payments	Social media analytics (400,242 tweets)	TAM; UTAUT	/	Satisfaction with mobile payments
Khalilzadeh et al., 2017	Trust in NFC-based mobile payments	Survey (N = 412)	UTAUT	Perceived risk; Perceived security	Utilitarian performance expectancy; Hedonic performance expectancy; Effort expectancy
Leong et al., 2021	Trust in mobile payments	Survey (N = 469)	Trust-based acceptance model; Trust transfer theory	/	Trust in social commerce
Liébana-Cabanillas et al., 2014	Trust in mobile payments	Experiment (N = 2012)	TAM	Perceived risk; External influences	Perceived ease of use; Attitude
Lisana, 2021	Trust in mobile payments	Survey (N = 736)	TAM, UTAUT	Uncertainty avoidance; Network externalities; Social Influences	Perceived ease of use; Perceived usefulness; Behavioral intentions
Loh et al., 2020	Trust in mobile payments	Survey (N = 343)	Push-pull-mooring; Status quo bias	/	Intention to switch from cash to mobile payments
Lu et al., 2011	Trust in mobile payments	Survey (N = 374)	Valence framework	Trust in internet payment	Perceived risk; Relative advantage; Behavioral intention
Mallat, 2007	Trust in mobile payments service providers	Qualitative study (focus group interviews, N = 46)	/	/	Perceived risks; Adoption
Nwankpa and Datta, 2022	Trust in mobile payment platforms	Survey (N = 527)	Economic utility and trust	Mobile payment platform utility	Commitment; Perceived healthcare service quality
Ogbanufe and Kim, 2018	Trust in online stores	Experiment (N = 94)	Valence framework	Users who use fingerprint-based biometrics authentication payments express more trust in online stores than those who use credit cards only	/
Palash et al., 2022	Trust in FRP	Survey (N = 392)	Valence framework	/	Use intentions
Rouibah et al., 2016	Trust in online payments	Survey (N = 350)	Cognitive dissonance theory	Personal innovativeness; Propensity to trust; Familiarity; Presence of third-party seals; Perceived risk; Perceived enjoyment	Adoption intentions

(*continued on next page*)

Table 1 (*continued*)

Reference	Trust type	Research method	Theoretical lens	Trust antecedents	Trust consequences
Shao et al., 2019	Trust in mobile payment platforms	Survey (N = 740)	Innovation diffusion theory	Mobility; Customization; Security; Reputation	Perceived risk; Continuance intentions
Williams, 2021	Trust in mobile payments	Survey (N = 237)	TAM	/	Perceived risk; Use intentions
Yang et al., 2015	Trust in online payments	Survey (N = 870)	TRA, TPB, TAM, Decomposed theory of planned behavior	Perceived usefulness; Comparison; Total risk; Perceive ease of use	Use intentions
Yuan et al., 2020	Trust in mobile payments	Survey (N = 343)	SOR	Information quality; System quality; Service quality	Intimacy
Zhang et al., 2019	Trust in web payments	Survey (N = 552)	Value-based acceptance model	/	Perceived value of mobile payments
Zhou, 2011	Trust in mobile banking	Survey (N = 210)	/	Structural assurance; Information quality; System quality; Trust propensity	Perceived usefulness; Use intentions
Zhou, 2012	Trust in mobile banking	Survey (N = 210)	Elaboration likelihood model	Information quality; Service quality; System quality; Reputation; Structural assurance; Self-efficacy	/

Notes: FRP = facial recognition payment; NFC = near-field communication; SOR = stimuli-organism-response; TAM = technology acceptance model; TPB = theory of planned behavior; TRA = theory of reasoned action; UTAUT = unified theory of acceptance and use of technology.

According to a report by Nielsen Norman Group, the whole payment process only takes 10 to 15 s for new users, and for frequent users, it takes <10 s, much shorter than mobile payment based on QR-coding scanning (Liu, 2020). Second, it is entirely contactless; users need not touch anything (e.g., a mobile phone); they need only stand in front of the camera of an FRP device so that it can scan their face. Third, it is convenient, particularly when users forget to carry credit cards or mobile phones with them or when their hands are full with other purchased goods and they cannot enter a PIN or scan their fingerprint while making another purchase. Finally, FRP is safer than some traditional payment methods, such as using a password to authorize credit card or mobile payments. Particularly, FRP has evolved rapidly alongside the development of 3D cameras and artificial intelligence, and current FRP has been argued to be highly secure (Vazquez-Fernandez and Gonzalez-Jimenez, 2016).

On the other hand, FRP still raises concerns regarding uncertainty and risks for users, especially privacy and security concerns. First, FRP systems can be hacked. Photograph spoofing, video spoofing, 3D masks, and deep morphing are common techniques used in impersonation hacks (Cho and Jeong, 2017; Edmunds and Caplier, 2018; Li et al., 2018; Ryu et al., 2021; Yeung et al., 2020). Hackers can obtain targets' photographs or videos from non-FRP sources (e.g., social network sites) and present these images to an FRP system (Cho and Jeong, 2017). Although current FRP systems have adopted privacy-enhancing algorithms to counter 2D face hacks, 3D masks and deep morphing remain challenging as spoofing techniques (Li et al., 2018; Yeung et al., 2020). The evolution of 3D scanning and printing, as well as artificial intelligence in morphing, has supplied tools with which to accurately represent a target and facilitate the production of impersonation hacks. More methods of countering these hacks are needed to protect FRP users' privacy. Second, FRP providers can use or share collected facial information with the government or other surveillance companies (Yeung et al., 2020). Since FRP collects and stores high-quality facial information to ensure accuracy, the collected data can be used to identify people outside of FRP, such as in street cameras or workplace surveillance. Rules and regulations are needed to govern the collection, storage, and use of facial information and to protect users' privacy.

Thus, although FRP offers some advantages, privacy and security concerns might disrupt users' continuance intentions (Zhang and Kang, 2019). Users must build trust in FRP to reduce its related uncertainty and risks. Additionally, trust can facilitate long-term relationships between users, FRP technology, and FRP service providers—particularly through various FRP services or service providers. Hence, users' trust should play an important role in FRP continuance intentions. Therefore, the current study proposes and empirically examines a research model to understand the underlying mechanism of trust-building in FRP, as well as its effects on continuance intentions among FRP users.

2.2. Trust in payment technologies

In the IS field, *trust* is variably defined, but most definitions agree that its core is "an expectation from trustees to behave in a certain way when there is some uncertainty regarding these actions" (Turel et al., 2008, p. 125). Payment technologies involve different trustees, trust-building mechanisms, and outcomes. Specifically, payment technologies involve two main types of trustees. First, a payment technology can be trusted or distrusted because users are concerned about its ability to provide trustworthy, secure, and authentic financial services (Gong et al., 2020; Lu et al., 2011). Second, a service provider can be trusted or distrusted since users also care about its competence, benevolence, and integrity (Turel et al., 2008). In the current research context, *competence* refers to a service provider's ability to perform a task required by a payment technology's users, *benevolence* refers to service providers' caring about acting in users' best interest, and *integrity* describes service providers who are honest, and honor promises to their users (McKnight et al., 2002; Turel et al., 2008).

Trust-building mechanisms comprise three main streams: knowledge-based, institution-based, and trust-transfer mechanisms (Gong et al., 2020). Knowledge-based mechanisms, also called *technology-based mechanisms*, imply that users' trust in payment technologies is formed by their assessment of prior experiences using such technologies, such as perceived ease of use (Yang et al., 2015), perceived utility (Nwankpa and Datta, 2022), perceived security (Khalilzadeh et al., 2017), and perceived risk (Hu et al., 2021; Khalilzadeh et al., 2017). *Institution-based mechanisms* imply that a set of institutional assurances influences user trust in payment technologies, such as firm reputation and structural assurance (Shao et al., 2019; Zhou, 2012, 2011). *Trust transfer mechanisms* imply that users' trust in payment technologies is transferred from a relative source object; for instance, users' trust in online payments could positively affect their trust in mobile payments (Cao et al., 2018; Gong et al., 2020).

Prior literature has found that user trust in payment technologies produces different outcomes, which can be summarized into two main streams: *user cognition* and *behavior regarding payment technologies*. Specifically, user trust has been found to update users' cognitive assessments of payment technologies, such as perceptions regarding usefulness (Lisana, 2021; Zhou, 2011), ease of use (Liébana-Cabanillas et al., 2014; Lisana, 2021), benefits (Chin et al., 2022; Gao and Waechter, 2017), and risks (Shao et al., 2019; Williams, 2021). Moreover, user trust in payment technologies can directly facilitate users' behavioral intentions, such as adoption intentions (Franque et al., 2022; Gong et al., 2020) and continuance intentions (Franque et al., 2022; Shao et al., 2019). Table 1 summarizes prior studies on trust in payment technologies in the IS field.

In summary, prior studies on trust in the payment technologies context have primarily focused on trust in technology, and few studies have investigated building users' trust in payment technologies from a perspective integrating both technology- and institution-based mechanisms or the relationship between these two different trust types. Moreover, most prior studies have focused on how user trust influences the adoption of new payment technologies, and little attention has been paid to users' continuance intentions regarding FRP. Hence, the current study aims to investigate trust in both FRP itself and service providers, exploring these trust types' impact on continuance intentions from a perspective that integrates technology- and institution-based mechanisms.

3. Research model and hypotheses

User trust is important in explaining continuance intentions concerning innovative payment technologies (Cao et al., 2018; Franque et al., 2022). Based on prior findings on user trust in payment technologies, we proposed that users' FRP continuance intentions are affected by both technology-based trust (i.e., trust in FPR) and institution-based trust (i.e., trust in FRP service providers). Additionally, technology-based trust is determined by individuals' perceptions of privacy and security issues, which are crucial in the FPR context, including perceived vulnerability, response efficacy, and security. Furthermore, we proposed a relationship between these two different types of trust. Table 2 presents the constructs used in our research model.

Perceived vulnerability describes the chance of a privacy threat (Boss et al., 2015; Johnston and Warkentin, 2010). FRP is determined by users' facial information, which is vulnerable to potential hacks and surveillance (Li et al., 2018; Yeung et al., 2020). Specifically, current face recognition technologies can easily capture peoples' facial information through widespread digital tools or cameras without their consent, such as through photos on social network sites, street cameras, and airport cameras. Using spoofing techniques (e.g., 3D masks and deep morphing), collected facial information from non-FRP sources can be used to compromise FRP systems (Edmunds and Caplier, 2018; Li et al., 2018; Yeung et al., 2020). Additionally, the facial information collected by FRP is high-quality, and it can be used to identify and surveil people in public areas, such as workplaces and airports (Yeung et al., 2020). These problems increase users' sense of vulnerability when using FRP, which may reduce trust in this payment technology. Conversely, if FRP users do not perceive themselves as vulnerable to privacy risks, they will likely trust FRP. Therefore, we proposed the following hypothesis:

H1: Perceived vulnerability is negatively associated with trust in FRP.

Perceived response efficacy reveals users' belief that FRP's preventive measures protect their privacy effectively and sufficiently (Boss et al., 2015; Johnston and Warkentin, 2010). Various techniques have been used to improve face recognition's accuracy and efficiency (e.g., 3D approaches) and protect users' facial information (e.g., encryption algorithms or artificial intelligence) (Adjabi et al., 2020; Khan et al., 2021). For instance, the latest versions of FRP devices (e.g., the WeChat Frog and Alipay Dragonfly) are equipped with 3D infrared cameras that can perform live body detection, possibly avoiding identity fraud using fake faces (e.g., photos or 2D masks) (Alipay, 2022; WeChat Pay, 2022). Moreover, WeChat and Alipay have used privacy-enhancing technologies, such as differential anonymization, to encrypt original facial information, which can protect users' facial information (Alipay, 2022; WeChat Pay, 2022). Furthermore, they isolate encrypted facial information and other sensitive information (e.g., personal bank accounts) and store them separately, which can prevent unauthorized access (Alipay, 2022; WeChat Pay, 2022). These preventive measures may increase trust in FRP. While users with high response efficacy tend to assess FRP as trustworthy in providing reliable, safe financial services, users with low perceived response efficacy may feel uncertain and perceive threats to privacy protection, struggling to trust FRP as a secure and reliable approach to billing and payment. Therefore, we proposed the following hypothesis:

H2: Perceived response efficacy is positively associated with trust in FRP.

Perceived security reflects users' perceptions that FRP can securely transmit sensitive information, including users' financial and facial information (Shao et al., 2019; Zhang and Kang, 2019). Potential hacks to users' monetary and facial information raise users' concerns regarding finance and privacy risks, sparking security concerns. A strong sense of security can mitigate these risks, increasing users' trust in FRP (Khalilzadeh et al., 2017; Pavlou et al., 2007). The IS literature has identified perceived security as a significant determinant of trust. For instance, Flavián and Guinalíu (2006) found that users' perceived security is a critical factor influencing their trust in a website. Mobile payment research has reported that perceived security positively affects users' trust in mobile payments (Chin et al., 2022; Khalilzadeh et al., 2017; Shao et al., 2019). Similarly, in the FRP context, when users believe FRP is a secure approach to billing and payment, they tend to trust the technology. Therefore, we proposed the following hypothesis:

H3: Perceived security is positively associated with trust in FRP.

According to trust transfer theory, users' trust in an unknown target can transfer from a related source and only if a strong relationship between the target and source has been confirmed (Stewart, 2003). If users trust the known source and perceive such a close source-target relationship, then trust in the source will likely transfer to the target (Gong et al., 2020; Stewart, 2006). In China, FRP services are primarily offered by two famous payment technologies: Alipay and WeChat Pay. Additionally, FRP and FRP service providers are clearly and closely related. As a result, users' trust in these two FRP companies may transfer to FRP technology. Prior research has found that users' trust in an offline bank significantly influences their perceptions of that bank's online banking (Lee et al., 2007). Moreover, Franque et al. (2022) found that user trust in mobile payment technology is influenced by benevolence, competence, and integrity, which represent user trust in service providers. Therefore, we assumed that trust in FRP service providers affects user

Table 2
Construct definitions.

Construct	Definition
Continuance intention	Users' willingness to continue using FRP (Bhattacherjee, 2001)
Perceived response efficacy	Users' perceptions of how effectively an FRP safeguards their private facial information (Posey et al., 2015)
Perceived security	Users' perceptions of how securely an FRP transmits financial information (Cheng et al., 2006)
Perceived vulnerability	Users' perceptions of the likelihood that their private facial information will be threatened (Posey et al., 2015)
Trust in FRP	Users' perceptions of an FRP's ability to provide trustworthy, secure, and authentic financial services (Gong et al., 2020)
Trust in a FRP service provider	Users' perceptions of a service provider's integrity, competence, and benevolence (Turel et al., 2008)

Note: FRP = facial recognition payment.

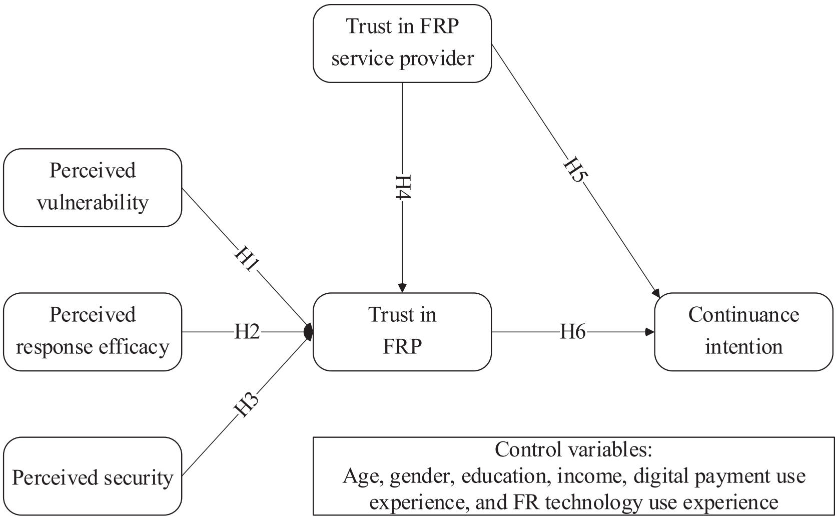
Trust in FRP service provider
Perceived vulnerability
Perceived response efficacy
Perceived security
Trust in FRP
Continuance intention
H1
H2
H3
H4
H5
H6
Control variables:
Age, gender, education, income, digital payment use experience, and FR technology use experience

Fig. 1. Research model.

trust in FRP technology. Hence, we proposed the following hypothesis:

H4: Trust in a service provider is positively associated with trust in FRP.

Trust in a service provider represents users' belief that FRP service providers have user-beneficial attributes, such as competency (the ability to meet FRP users' needs), benevolence (acting in the best interest of FRP users), and integrity (honesty and promise-keeping for FRP users) (Bhattacherjee, 2002; McKnight et al., 2002). Trust in service providers has been demonstrated to motivate individuals' use intentions concerning payment technologies. For instance, in a qualitative study on mobile payments, Mallat (2007) demonstrated that trust in service providers is an important factor affecting users' adoption of mobile payments. Luo et al. (2010) found that user trust in a bank positively affects users' intentions to use that bank's mobile banking services. Therefore, we assumed that, if users trust FRP service providers, they tend to continue using FRP. Accordingly, we developed the following hypothesis:

H5: Trust in a service provider is positively associated with continuance intentions.

Trust in FRP reflects users' beliefs about FRP's ability to provide trustworthy, secure, and authentic financial services (Gong et al., 2020; Luo et al., 2010). Such trust helps users reduce risks and ensure payment success when using FRP, increasing intentions to use FRP (Gong et al., 2020; Luo et al., 2010). Prior studies have shown that trust in payment technologies positively influences individuals' behavioral intentions. For instance, Gong et al. (2020) found that both cognitive and emotional trust in mobile payments positively influences intentions to use this payment technology. Franque et al. (2022) found that users' overall trust in mobile payments facilitates their continuance intentions. Likewise, in the FRP context, if users trust FRP financial services as secure, assured, and truthful, they will likely use FRP continually. Hence, we developed the following hypothesis:

H6: Trust in FRP is positively associated with continuance intentions.

Finally, user characteristics—such as age, gender, education, income, and prior experience using payment technologies—have been cited as essential control variables when studying individuals' behavioral intentions concerning new payment technologies (Chin et al., 2022; Hu et al., 2021). Also, users' prior experience using face recognition technology might influence such intentions (Venkatesh et al., 2012, 2003). Therefore, we tested age, gender, education, income, prior digital payment use experience (e.g., the web or mobile payments), and prior face recognition use experience outside FRP settings (e.g., airports) as control variables in this study. Fig. 1 presents our research model.

4. Research methodology

4.1. Instrument development

This study employed previously validated scales to ensure the reliability and validity of the instruments used for each construct included in our research model. A seven-point Likert scale, ranging from "strongly disagree" to "strongly agree," was used to measure all constructs. Specifically, this study measured trust in FRP by adopting items from the study by Kim et al. (2009). To measure continuance intentions, perceived response efficacy, perceived security, perceived vulnerability, and trust in service providers, we used items from the works of Bhattacherjee (2001), Posey et al. (2015), Cheng et al. (2006), Johnston and Warkentin (2010), and Turel et al. (2008), respectively. All items for each construct were revised to fit the FRP context. The complete list of measurement items for the constructs included in our model is presented in the Appendix.

4.2. Data collection

An online survey was conducted to collect empirical data in China via the China-based consulting company Wenjuanxing. The survey targeted a sample of users of the two dominant FRP companies: Alipay and WeChat Pay. The questionnaire was created in English since most constructs were measured by adapting previously validated scales from international journals. Then, the questionnaire was translated into Chinese by the authors, who are fluent in both English and Chinese. To ensure content and translation validity, a pilot test was conducted, gathering feedback on the questionnaire. Several sentences were revised to make their description clearer, and some questions were reordered to make the survey's structure more cohesive. Then, the finalized questionnaire was sent to target respondents in China via Wenjuanxing's sample service.

The questionnaire comprised three sections. It began with a consent form. Each respondent was informed about the aim of the research, the voluntary nature of participation, the confidentiality of the collected data, and the contact information of the researchers. If a prospective respondent agreed to participate, they had to sign a consent form and then complete the online questionnaire. Respondents needed to answer questions regarding their demographic information (e.g., age, gender, and education), prior experience using digital payment services provided by Alipay and WeChat Pay (e.g., web payments or mobile payments), prior experience using facial recognition technology beyond FRP (e.g., device authentication or facial recognition for airport check-ins and check-outs), and their experience using FRP provided by Alipay and WeChat Pay. Then, respondents reported their opinions and perceptions about using FRP in their daily lives. Each respondent who completed the online questionnaire received incentive compensation, such as a digital red packet with money ranging from 1 to 5 Renminbi (RMB). Three attention-check questions were incorporated into the survey to ensure that respondents were sufficiently attentive, such as, "Please select 'disagree' on this seven-point Likert scale." Table 3 presents respondents' basic information.

4.3. Common method variance

This study used Harman's single-factor test (Podsakoff et al., 2003) to test common method variance. The results of this test showed that the greatest total variance for any factor was 38.366 %, which was lower than 40 %, so common method variance seems not to have been a critical concern in this study. Additionally, the results of a full collinearity test showed that the values of variance inflation factors (VIFs) ranged from 1.298 to 3.247, which was lower than 3.3, indicating that collinearity was not a serious concern in this study (Kock, 2015).

Table 3
Respondent demographics.

Items	Type	Number	Percentage
Age (years)	18–25	43	19.8
	26–35	120	55.3
	36–45	37	17.1
	46–55	15	6.9
	>55	2	0.9
Gender	Male	149	68.7
	Female	67	30.9
	Unwilling to answer	1	0.5
Education	Junior high school	2	0.9
	High school	9	4.1
	Junior college	23	10.6
	Bachelor	162	74.7
	Master	21	9.7
Income (Renminbi, RMB)	≤15,000	25	11.5
	15,001–25,000	21	9.7
	25,001–35,000	13	6.0
	35,001–45,000	11	5.1
	45,001–55,000	26	12.0
	>55,000	121	55.8
Experience using web or mobile payments	≤1 year	6	2.8
	2–3 years	57	26.3
	4–5 years	60	27.6
	>5 years	94	43.3
Experience using face recognition technology	Never	8	3.7
	Actively use	152	70.0
	Passively use	57	26.3

4.4. Data analysis and results

4.4.1. Measurement model

We used SmartPLS 3.0 to test both measurement and structural models. The measurement model was tested by assessing convergent validity and discriminant validity. Specifically, factor loadings, Cronbach's alpha (CA), composite reliability (CR), and average variance extracted (AVE) were used to assess convergent validity (Fornell and Larcker, 1981; Tenenhaus et al., 2005). As Table 4 shows, two items (PRE1 and TISP5) were removed because their factor loading values were below 0.7; other items' factor loadings exceeded 0.7. The CA values of all constructs were between 0.701 and 0.916, which exceeded the suggested value of 0.7. CR

Table 4
Convergent validity test results.

	Items	Factor loading	CA	CR	AVE
Continuance intentions (CI)	CI1	0.846	0.780	0.872	0.694
	CI2	0.805			
	CI3	0.847			
Perceived response efficacy (PRE)	PRE2	0.782	0.701	0.827	0.614
	PRE3	0.755			
	PRE4	0.813			
Perceived security (PS)	PS1	0.847	0.841	0.893	0.676
	PS2	0.782			
	PS3	0.843			
	PS4	0.816			
Trust in FRP (TIF)	TIF1	0.879	0.878	0.924	0.803
	TIF2	0.900			
	TIF3	0.909			
Trust in a service provider (TISP)	TISP1	0.826	0.781	0.857	0.600
	TISP2	0.737			
	TISP3	0.756			
	TISP4	0.777			
Perceived vulnerability (PV)	PV1	0.930	0.916	0.947	0.855
	PV2	0.918			
	PV3	0.927			

Note: FRP = facial recognition payment; CA = Cronbach's alpha; CR = composite reliability; AVE = average variance extracted.

Table 5
Cross-loading test results.

	CI	PRE	PS	TIF	TISP	PV
CI1	**0.846**	0.416	0.510	0.449	0.385	0.384
CI2	**0.805**	0.404	0.452	0.382	0.376	0.259
CI3	**0.847**	0.506	0.503	0.489	0.426	0.330
PRE2	0.452	**0.782**	0.461	0.454	0.402	0.259
PRE3	0.368	**0.755**	0.442	0.430	0.405	0.307
PRE4	0.433	**0.813**	0.522	0.497	0.513	0.394
PS1	0.514	0.517	**0.847**	0.616	0.520	0.553
PS2	0.489	0.464	**0.782**	0.445	0.505	0.357
PS3	0.474	0.507	**0.843**	0.531	0.505	0.496
PS4	0.457	0.508	**0.816**	0.559	0.571	0.468
TIF1	0.491	0.533	0.529	**0.879**	0.498	0.344
TIF2	0.437	0.482	0.555	**0.900**	0.521	0.400
TIF3	0.497	0.564	0.681	**0.909**	0.563	0.523
TISP1	0.505	0.494	0.616	0.547	**0.826**	0.405
TISP2	0.283	0.365	0.465	0.379	**0.737**	0.226
TISP3	0.335	0.414	0.422	0.389	**0.756**	0.262
TISP4	0.302	0.456	0.440	0.478	**0.777**	0.292
PV1	0.397	0.399	0.543	0.447	0.358	**0.930**
PV2	0.311	0.312	0.516	0.405	0.379	**0.918**
PV3	0.374	0.422	0.542	0.466	0.362	**0.927**

Notes: CI = continuance intentions; PRE = perceived response efficacy; PS = perceived security; TIF = trust in facial recognition payment; TISP = trust in a service provider; PV = perceived vulnerability. The numbers in bold represent item loadings on their respective assigned latent variables.

Table 6
Correlations and square roots of Average Variance Extracted (AVE).

	CI	PRE	PS	TIF	TISP	PV
Continuance intentions (CI)	0.833					
Perceived response efficacy (PRE)	0.534	0.784				
Perceived security (PS)	0.587	0.608	0.822			
Trust in FRP (TIF)	0.532	0.589	0.661	0.896		
Trust in a service provider (TISP)	0.476	0.564	0.639	0.590	0.775	
Perceived vulnerability (PV)	0.392	0.411	0.578	0.476	0.395	0.925

Note: FRP = facial recognition payment.

Table 7
The heterotrait-monotrait ratio of correlations (HTMT) test results.

	CI	PRE	PS	TIF	TISP	PV
Continuance intention (CI)						
Perceived response efficacy (PRE)	0.724					
Perceived security (PS)	0.724	0.796				
Trust in FRP (TIF)	0.636	0.755	0.755			
Trust in service provider (TISP)	0.585	0.756	0.771	0.695		
Perceived vulnerability (PV)	0.458	0.512	0.648	0.524	0.452	

Note: FRP = facial recognition payment.

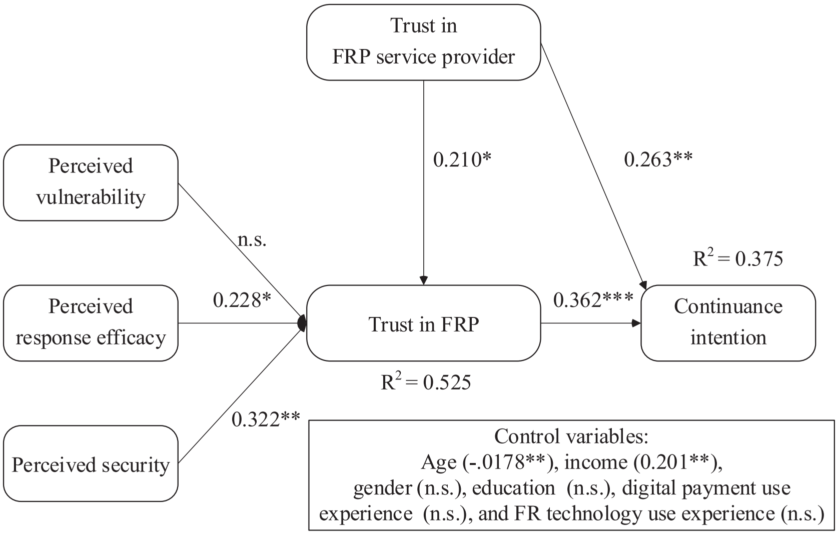
Trust in FRP service provider
0.210*
0.263**
Perceived vulnerability
n.s.
$R^2 = 0.375$
Perceived response efficacy
0.228*
Trust in FRP
0.362***
Continuance intention
$R^2 = 0.525$
0.322**
Perceived security
Control variables:
Age (-.0178**), income (0.201**),
gender (n.s.), education (n.s.), digital payment use
experience (n.s.), and FR technology use experience (n.s.)

Fig. 2. Partial Least Squares (PLS) path modeling results.

values ranged from 0.827 to 0.947, exceeding the recommended value of 0.7. AVE values ranged from 0.600 to 0.855, exceeding 0.5. Therefore, convergent validity was established in this study (Fornell and Larcker, 1981; Tenenhaus et al., 2005).

To evaluate discriminant validity, the cross-loading of each indicator (Chin, 1998), Fornell–Larcker criterion (Fornell and Larcker, 1981), and the heterotrait–monotrait ratio of correlation (HTMT) (Henseler et al., 2015) were tested. As Table 5 shows, the factor-loading of each indicator for its relevant construct exceeded the cross-loadings of the other constructs. Additionally, each construct's correlations with other constructs were lower than the square root of its AVE (see Table 6). Moreover, as Table 7 shows, HTMT values ranged from 0.452 to 0.796, below 0.85. Therefore, discriminant validity was confirmed in this study.

4.4.2. *Structural model*

Our structural model was assessed by measuring path significance and our hypotheses' effects, predictive relevance (Q^2), and goodness of fit. The Partial Least Squares (PLS) path modeling results are depicted in Fig. 2.

Our model explained 37.5 % of the variance in FRP continuance intentions, and 52.5 % of the variance in trust in FRP itself. Both trust in a service provider ($\beta = 0.263$, $p < 0.01$) and trust in FRP itself ($\beta = 0.362$, $p < 0.001$) significantly positively influenced continuance intentions. Trust in a service provider influenced trust in FRP significantly ($\beta = 0.210$, $p < 0.05$). Perceived response efficacy ($\beta = 0.228$, $p < 0.05$) and perceived security ($\beta = 0.322$, $p < 0.01$) significantly affected trust in FRP itself. In contrast, perceived vulnerability exerted no significant influence on trust in FRP. Therefore, H2, H3, H4, H5, and H6 were supported, while H1 was not.

The Stone–Geisser Q^2 was further used to estimate the research model's predictive relevance (Geisser, 1974; Hair et al., 2017; Stone, 1974). The result showed that the Q^2 values of continuance intentions, and trust in FRP itself were 0.226 and 0.401, respectively, which suggested good predictive relevance (Hair et al., 2017).

This study also used the standardized root mean square residual (SRMR) to evaluate our research model's goodness of fit (Hair et al., 2017; Henseler et al., 2014). The result of this evaluation was 0.065, which was lower than the threshold of 0.08 suggested by Hu and Bentler (1999), indicating a good fit.

Among the control variables, age ($\beta = -0.178$, $p < 0.01$) and income ($\beta = 0.201$, $p < 0.01$) significantly influenced continuance intentions, whereas gender, education, digital payment use experience, and face recognition technology use experience had no significant impact.

5. Discussion

Our findings raise some interesting points. First, as expected, users' FRP continuance intentions are significantly and positively affected by both institution-based trust (i.e., trust in a service provider) and technology-based trust (i.e., trust in FRP). Our findings on the former relationship are consistent with findings in mobile payment research (Mallat, 2007; Shao et al., 2019). Users' trust in a service provider significantly influences their intentions to continue using FRP. Our findings on the significant relationship between trust in FRP and continuance intentions also align with previous research. For instance, Franque et al. (2022) demonstrated that users' overall trust in mobile payments is significantly related to user continuance intentions. Similarly, in the FRP context, when users feel that FRP is trustworthy and that an FRP service provider also keeps their promises and honors their commitments, they will likely continue using FRP. These findings indicate that trust-building in the FRP context involves two different levels—institution- and technology-based—which should be considered in future research.

Second, this study found that institution-based trust (i.e., trust in a service provider) significantly positively influences technology-based trust (i.e., trust in FRP). This finding indicates that trust in providers will induce trust in their developed products through the trust transfer mechanism (Stewart, 2006, 2003). When users trust a payment technology company, they will likely assess their product as trustworthy, such as FRP in the current study.

Third, our study found that users' trust in FRP is affected by a privacy-related factor—namely, their perceptions related to response efficacy. This finding indicates that privacy issues significantly influence user trust in FRP. The more privacy protection in FRP users perceive, the stronger they trust FRP. This finding might be explained by people's worries about the leakage and misuse of their facial information since changing such unique identifiers is difficult for users (Liu et al., 2021; Yeung et al., 2020). When users believe FRP strategies and techniques can protect their private facial information effectively and sufficiently, they will likely trust this new payment technology.

Surprisingly, the other privacy-related factor that we examined—perceived vulnerability—does not significantly influence trust in FRP. This finding is not consistent with some findings regarding mobile banking services in prior research. For instance, Khoa (2021) found that users' perception of vulnerability has a negative influence on their trust in mobile banking via perceived value. A possible reason for the insignificant effect of perceived vulnerability on trust in FRP is that when users trust the FRP service providers, they are more likely to endure a high level of vulnerability regarding privacy issues. Even though the probability of being exposed to a privacy threat is high, users trust the FRP provider's service is secure and trustworthy, thereby, their perceived vulnerability may lose its importance in affecting their trust in FRP itself. This insignificant relationship between perceived vulnerability and trust in FRP also indicates that, despite privacy issues' importance in the FRP context, when unfolding the components of privacy issues, not every privacy-related factor will significantly influence user trust in FRP. This finding calls for further investigations to better explain the complex nature of relationships between privacy and trust in the FRP context.

Finally, this study found a positive relationship between perceived security and trust in FRP, consistent with previous research on payment technologies. For instance, mobile payment research found that users' perceptions of security significantly influence their trust in this technology (Chin et al., 2022; Khalilzadeh et al., 2017). In the FRP context, when users perceive FRP as a safe, secure tool for billing and payment, they will likely trust this new payment method.

6. Conclusion

6.1. Theoretical contributions

This study enriches the FRP literature by investigating the roles of different types of trust in determining users' continuance intention to use FRP. Our findings offer several theoretical contributions. First, recent studies on FRP have focused mainly on initial adoption (Hu et al., 2021; Moriuchi, 2021; Palash et al., 2022) but largely ignored continuance intentions, which are crucial to FRP's long-term success. This study has filled this research gap by examining trust-building in the FRP context from the views of FRP service providers and FRP technologies and by examining the antecedents of trust in FRP technologies from a privacy and security perspective. Our findings indicate that both trust in FRP and trust in service providers positively affect users' continuance intentions concerning FRP, suggesting that the antecedents of continuous FRP use can be well understood from a trust-based perspective.

Second, this study enriches the trust literature by examining the relationship between trust in technologies and institutions in FRP use, which yields new insights into the mechanism underlying trust building from the relationships of different types of trust in payment technology use. Unlike prior studies on trust in payment technologies mainly adopted either technology-based perspectives (e.g., Cao et al., 2018; Chin et al., 2022) or institution-based perspectives (e.g., Mallat, 2007; Shao et al., 2019), our study has integrated these two different types of trust and examined their relationship. Our study suggests that users' trust in service providers can trigger their trust in FRP, indicating the interdependence between different types of trust.

Third, this study offers an understanding of the determinants of trust in FRP from a privacy and security perspective, which is highly relevant and important in the FRP context. Unlike prior studies on the antecedents of trust in payment technologies, which have mainly adopted a technology-based perspective, such as by focusing on the quality of information, a system, and service (e.g., Gao and Waechter, 2017; Yuan et al., 2020), or the benefits of payment technologies, such as perceived ease of use (e.g., Yang et al., 2015) and perceived value (e.g., Hu et al., 2021), or a trust transfer from one payment technology to another payment technology (e.g., Cao et al., 2018; Gong et al., 2020), this study enriches the trust literature by examining the roles of both privacy and security issues in building user trust in FRP and by revealing the roles of different privacy- and security-related factors in explaining trust in FRP, such as perceived vulnerability, perceived response efficacy, and perceived security. The significant impacts of perceived response efficacy and perceived security on users' trust in FRP indicate the importance of building user trust in RFP from the view of privacy and security protection perspective.

Lastly, though users' perceived privacy has been identified as a crucial barrier to user trust in payment technologies, prior research has only examined privacy from a general perspective (e.g., Chin et al., 2022). This study advances the understanding of the impact of privacy on trust by examining the roles of privacy's components in explaining user trust in FRP. The findings on the insignificant impact of perceived vulnerability and the significant impacts of perceived response efficacy and perceived security on users' trust in FRP provide a comprehensive understanding of the different roles of privacy's components in explaining trust in FRP.

6.2. Practical implications

This study may also offer practical implications to FRP service providers concerning how to facilitate user trust and promote FRP continuance intentions among individual users. First, our findings on the positive influence of trust in both FRP itself and FRP service providers suggest that FRP service providers develop these two types of user trust to promote users' continuance intentions. Specifically, our findings on the positive influence of perceived response efficacy and security on trust in FRP suggest that service providers should focus on improving users' perceptions of privacy protection and security to enhance users' trust in FRP. This enhancement can be achieved by updating FRP privacy protection techniques, such as by using artificial intelligence to encrypt originally collected facial data and by updating 3D camera technology to avoid identity fraud caused by fake faces. Additionally, FRP service providers could offer users clear, detailed explanations about FRP's privacy-protecting design to show them that their facial information cannot be easily hacked and will be used under strict measures. Furthermore, FRP service providers could provide users with sufficient payment documentation to show that FRP transactions are reliable and secure.

We also recommend, given our findings on the relationship between trust in FRP itself and trust in service providers, that FRP service providers recognize the significance of user trust. Although FRP companies in China (such as Alipay and WeChat) have offered payment technologies for many years and are widely recognized by consumers, maintaining user trust in FRP companies remains important since this type of trust can trigger user trust in technology products, as our findings suggest.

6.3. Limitations and future research directions

This study faced the following limitations. First, we collected data to test our research model in China alone. Future work could enlarge our sample size to different countries, increasing the generalizability of our findings. Second, since FRP is developing rapidly in China, the data we collected via survey may not fully reflect the technology's complex features. Future research could consider mixed approaches (i.e., qualitative and quantitative methods) to expand upon our explanation of the antecedents to trust and continuance intentions in the FRP context. Third, this study examined the determinants of trust in FRP from only privacy- and security-based perspectives and has not considered the beneficial factors related to FRP, which could be closely associated with trust in FRP. Therefore, future research could also consider the benefits of FRP use as potential antecedents of trust in FRP, such as perceived usefulness, perceived ease of use, perceived value, perceived convenience, or perceived novelty.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The authors do not have permission to share data.

Appendix. Construct measurements

Construct	Instrument	Reference
Continuance intentions	• I intend to continue using facial recognition payments (FRP), rather than discontinuing their use. • My intentions are to continue using FRP, rather than using any alternative means (cash or mobile payments). • If I could, I would like to continue my use of FRP.	(Bhattacherjee, 2001)
Perceived security	• I would feel secure billing using FRP. • FRP is a secure billing means even though my sensitive information is used by the FRP. • I would feel totally safe billing using FRP even though they need my sensitive information. • Overall, FRP is a safe means to transmit sensitive information.	(Cheng et al., 2006)
Perceived response efficacy	• The FRP device is equipped with a 3D infrared camera that can perform live body detection, which can effectively avoid identity fraud caused by various fake faces (e.g., photos or masks). • FRP uses privacy-enhancing technologies, such as differential privacy or anonymization, to encrypt the original facial information, which can effectively protect my facial information. • FRP isolates encrypted facial information and other private information (e.g., personal account) and stores them separately, which can effectively stop people from accessing my private information. • The FRP service providers' efforts to keep my facial information safe from information security threats are effective.	(Posey et al., 2015)
Trust in FRP	• FRP always provides accurate financial services. • FRP always provides reliable financial services. • FRP always provides safe financial services.	(Kim et al., 2009)
Trust in service provider	• The FRP service provider is trustworthy. • I trust the FRP service provider keeps my best interests in mind. • The FRP service provider will keep the promises it makes to me. • I believe in the information that the FRP service provider offers me. • The FRP provider wants to be known as a provider that keeps promises and honors commitments.	(Turel et al., 2008)
Perceived vulnerability	• When using FRP, my facial information is at risk of being invaded. • When using FRP, it is likely that my facial information will be invaded. • When using FRP, it is possible that my facial information will be invaded.	(Johnston and Warkentin, 2010)

References

Adjabi, I., Ouahabi, A., Benzaoui, A., Taleb-Ahmed, A., 2020. Past, present, and future of face recognition: A review. Electron. 9, 1–53. https://doi.org/10.3390/electronics9081188.

Alipay, 2022. The introduction of dragonfly. URL: https://cn.aliyun.com/daily-act/dragonfly (accessed 4.12.22).

Bhattacherjee, A., 2001. Understanding information systems continuance: an expectation-confirmation model. MIS Q. 25, 351–370. https://doi.org/10.2307/3250921.

Bhattacherjee, A., 2002. Individual trust in online firms: Scale development and initial test. J. Manag. Inf. Syst. 19, 211–241. https://doi.org/10.1080/07421222.2002.11045715.

Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D., Polak, P., 2015. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS Q. 39, 837–864. 10.25300/MISQ/2015/39.4.5.

Cao, X., Yu, L., Liu, Z., Gong, M., Adeel, L., 2018. Understanding mobile payment users' continuance intention: a trust transfer perspective. Internet Res. 28, 456–476. https://doi.org/10.1108/IntR-11-2016-0359.

Cheng, T.C.E., Lam, D.Y.C., Yeung, A.C.L., 2006. Adoption of internet banking: An empirical study in Hong Kong. Decis. Support Syst. 42, 1558–1572. https://doi.org/10.1016/j.dss.2006.01.002.

Chin, A.G., Harris, M.A., Brookshire, R., 2022. An empirical investigation of intent to adopt mobile payment systems using a trust-based extended valence framework. Inf. Syst. Front. 24, 329–347. https://doi.org/10.1007/s10796-020-10080-x.

Chin, W.W., 1998. The partial least squares approach to structural equation modelling. In Marcoulides G. A. (Ed.). Mod. Methods Bus. Res. 295, 295–336.

Cho, M., Jeong, Y., 2017. Face recognition performance comparison between fake faces and live faces. Soft Comput. 21, 3429–3437. https://doi.org/10.1007/s00500-015-2019-4.

Dang, V.T., Nguyen, N., Nguyen, H.V., Nguyen, H., Van Huy, L., Tran, V.T., Nguyen, T.H., 2022. Consumer attitudes toward facial recognition payment: an examination of antecedents and outcomes. Int. J. Bank Mark. 40, 511–535. https://doi.org/10.1108/IJBM-04-2021-0135.

Edmunds, T., Caplier, A., 2018. Motion-based countermeasure against photo and video spoofing attacks in face recognition. J. Vis. Commun. Image Represent. 50, 314–332. https://doi.org/10.1016/j.jvcir.2017.12.004.

Flavián, C., Guinalíu, M., 2006. Consumer trust, perceived security and privacy policy. Ind. Manag. Data Syst. 106, 601–620. https://doi.org/10.1108/02635570610666403.

Fornell, C., Larcker, D.F., 1981. Structural equation models with unobservable variables and measurement error: algebra and statistics. J. Mark. Res. 18, 382–388. https://doi.org/10.2307/3150980.

Franque, F.B., Oliveira, T., Tam, C., 2022. Continuance intention of mobile payment: TTF model with trust in an African context. Inf. Syst. Front. 5, 1–19. https://doi.org/10.1007/s10796-022-10263-8.

Gao, L., Waechter, K.A., 2017. Examining the role of initial trust in user adoption of mobile payment services: an empirical investigation. Inf. Syst. Front. 19, 525–548. https://doi.org/10.1007/s10796-015-9611-0.

Geisser, S., 1974. A predictive approach to the random effect model. Biometrika 61, 101–107. https://doi.org/10.2307/2334290.

Gong, X., Zhang, K.Z.K., Chen, C., Cheung, C.M.K., Lee, M.K.O., 2020. What drives trust transfer from web to mobile payment services? The dual effects of perceived entitativity. Inf. Manag. 57, 103250 https://doi.org/10.1016/j.im.2019.103250.

Hair, J.F., Hult, G.T.M., Ringle, C.M., Sarstedt, M., 2017. A primer on partial least squares structural equation modeling (PLS-SEM), Second. ed. SAGE Publications, Los Angeles.

Henseler, J., Dijkstra, T.K., Sarstedt, M., Ringle, C.M., Diamantopoulos, A., Straub, D.W., Ketchen, D.J., Hair, J.F., Hult, G.T.M., Calantone, R.J., 2014. Common beliefs and reality about PLS: comments on Rönkkö and Evermann (2013). Organ. Res. Methods 17, 182–209. https://doi.org/10.1177/1094428114526928.

Henseler, J., Ringle, C.M., Sarstedt, M., 2015. A new criterion for assessing discriminant validity in variance-based structural equation modeling. J. Acad. Mark. Sci. 43, 115–135. https://doi.org/10.1007/s11747-014-0403-8.

Hillman, S., Neustaedter, C., 2017. Trust and mobile commerce in North America. Comput. Human Behav. 70, 10–21. https://doi.org/10.1016/j.chb.2016.12.061.

Horswill, I., 2021. Facial recognition payments becoming more prevalent in major cities. accessed 4.10.22 CEO Mag. https://www.theceomagazine.com/business/innovation-technology/facial-recognition-payments/.

Hu, L., Bentler, P.M., 1999. Cutoff criteria for fit indexes in covariance structure analysis: conventional criteria versus new alternatives. Struct. Equ. Model. A Multidiscip. J. 6, 1–55. https://doi.org/10.1080/10705519909540118.

Hu, B., Liu, Y., Yan, W., 2021. Should I scan my face? The influence of perceived value and trust on Chinese users' intention to use facial recognition payment. Proceedings of 23rd Biennial Conference of the International Telecommunications Society (ITS). International Telecommunications Society (ITS), Calgary, Gothenburg, pp. 1–31.

iiMedia Report, 2019. Social value of the adoption of China face-scanning payment technology research report. URL: https://report.iimedia.cn/repo8-0/38932.html?acPlatCode=xq&acFrom=bg38932 (accessed 4.4.22).

Johnston, Warkentin, 2010. Fear appeals and information security behaviors: an empirical study. MIS Q. 34, 549–566. https://doi.org/10.2307/25750691.

Kar, A.K., 2021. What affects usage satisfaction in mobile payments? Modelling user generated content to develop the "digital service usage satisfaction model". Inf. Syst. Front. 23, 1341–1361. https://doi.org/10.1007/s10796-020-10045-0.

Khalilzadeh, J., Ozturk, A.B., Bilgihan, A., 2017. Security-related factors in extended UTAUT model for NFC based mobile payment in the restaurant industry. Comput. Human Behav. 70, 460–474. https://doi.org/10.1016/j.chb.2017.01.001.

Khan, F.A., Bouridane, A., Boussakta, S., Jiang, R., Almaadeed, S., 2021. Secure facial recognition in the encrypted domain using a local ternary pattern approach. J. Inf. Secur. Appl. 59, 1–5. https://doi.org/10.1016/j.jisa.2021.102810.

Khoa, B.T., 2021. The impact of the personal data disclosure's tradeoff on the trust and attitude loyalty in mobile banking services. J. Promot. Manag. 27, 585–608. https://doi.org/10.1080/10496491.2020.1838028.

Kim, G., Shin, B., Lee, H.G., 2009. Understanding dynamics between initial trust and usage intentions of mobile banking. Inf. Syst. J. 19, 283–311. https://doi.org/10.1111/j.1365-2575.2007.00269.x.

Kock, N., 2015. Common method bias in PLS-SEM: A full collinearity assessment approach. Int. J. e-Collaboration 11, 1–10. https://doi.org/10.4018/ijec.2015100101.

Lee, K.C., Kang, I., McKnight, D.H., 2007. Transfer from offline trust to key online perceptions: an empirical study. IEEE Trans. Eng. Manag. 54, 729–741. https://doi.org/10.1109/TEM.2007.906851.

Leong, B., 2019. Facial recognition and the future of privacy: I always feel like somebody's watching me. Bull. At. Sci. 75, 109–115. https://doi.org/10.1080/00963402.2019.1604886.

Leong, L.Y., Hew, T.S., Ooi, K.B., Chong, A.Y.L., Lee, V.H., 2021. Understanding trust in ms-commerce: The roles of reported experience, linguistic style, profile photo, emotional, and cognitive trust. Inf. Manag. 58, 103416 https://doi.org/10.1016/j.im.2020.103416.

Li, L., Correia, P.L., Hadid, A., 2018. Face recognition under spoofing attacks: Countermeasures and research directions. IET Biometrics 7, 3–14. https://doi.org/10.1049/iet-bmt.2017.0089.

Liébana-Cabanillas, F., Sánchez-Fernández, J., Muñoz-Leiva, F., 2014. Antecedents of the adoption of the new mobile payment systems: The moderating effect of age. Comput. Human Behav. 35, 464–478. https://doi.org/10.1016/j.chb.2014.03.022.

Lisana, L., 2021. Factors influencing the adoption of mobile payment systems in Indonesia. Int. J. Web Inf. Syst. 17 https://doi.org/10.1108/IJWIS-01-2021-0004.

Liu, F., 2020. Making cutting-edge technology approachable: a case study of facial-recognition payment in China. accessed 6.29.22 Nielsen Norman Gr. https://www.nngroup.com/articles/face-recognition-pay/.

Liu, Y. li, Yan, W., Hu, B., 2021. Resistance to facial recognition payment in China: The influence of privacy-related factors. Telecomm. Policy 45, 1–18. 10.1016/j.telpol.2021.102155.

Loh, X.-M., Lee, V.-H., Tan, G.-W.-H., Ooi, K.-B., Dwivedi, Y.K., 2020. Switching from cash to mobile payment: what's the hold-up? Internet Res. 31, 376–399. https://doi.org/10.1108/INTR-04-2020-0175.

Lu, Y., Yang, S., Chau, P.Y.K., Cao, Y., 2011. Dynamics between the trust transfer process and intention to use mobile payment services: A cross-environment perspective. Inf. Manag. 48, 393–403. https://doi.org/10.1016/j.im.2011.09.006.

Luo, X., Li, H., Zhang, J., Shim, J.P., 2010. Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. Decis. Support Syst. 49, 222–234. https://doi.org/10.1016/j.dss.2010.02.008.

Mallat, N., 2007. Exploring consumer adoption of mobile payments – A qualitative study. J. Strateg. Inf. Syst. 16, 413–432. https://doi.org/10.1016/j.jsis.2007.08.001.

McKnight, D.H., Choudhury, V., Kacmar, C., 2002. Developing and validating trust measures for e-commerce: An integrative typology. Inf. Syst. Res. 13, 334–359. https://doi.org/10.1287/isre.13.3.334.81.

Moriuchi, E., 2021. An empirical study of consumers' intention to use biometric facial recognition as a payment method. Psychol. Mark. 38, 1741–1765. https://doi.org/10.1002/mar.21495.

Nwankpa, J.K., Datta, P., 2022. Leapfrogging healthcare service quality in Sub-Saharan Africa: the utility-trust rationale of mobile payment platforms. Eur. J. Inf. Syst. 31, 40–57. https://doi.org/10.1080/0960085X.2021.1978339.

Ogbanufe, O., Kim, D.J., 2018. Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment. Decis. Support Syst. 106, 1–14. https://doi.org/10.1016/j.dss.2017.11.003.

Palash, M.A.S., Talukder, M.S., Islam, A.K.M.N., Bao, Y., 2022. Positive and negative valences, personal innovativeness and intention to use facial recognition for payments. Ind. Manag. Data Syst. 122, 1081–1108. https://doi.org/10.1108/IMDS-04-2021-0230.

Pavlou, Liang, Xue, 2007. Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. MIS Q. 31, 105–136. https://doi.org/10.2307/25148783.

Podsakoff, P.M., Mackenzie, S.B., Lee, J., Podsakoff, N.P., 2003. Common method biases in behavioral research: A critical review of the literature and recommended remedies. J. Appl. Psychol. 88, 879–903. https://doi.org/10.1037/0021-9010.88.5.879.

Posey, C., Roberts, T.L., Lowry, P.B., 2015. The impact of organizational commitment on insiders' motivation to protect organizational information assets. J. Manag. Inf. Syst. 32, 179–214. https://doi.org/10.1080/07421222.2015.1138374.

Premack, D., Woodruff, G., 1978. Does the chimpanzee have a theory of mind? Behav. Brain Sci. 1, 515–526. https://doi.org/10.1017/S0140525X00076512.

Rouibah, K., Lowry, P.B., Hwang, Y., 2016. The effects of perceived enjoyment and perceived risks on trust formation and intentions to use online payment systems: New perspectives from an Arab country. Electron. Commer. Res. Appl. 19, 33–43. https://doi.org/10.1016/j.elerap.2016.07.001.

Ryu, G., Park, H., Choi, D., 2021. Adversarial attacks by attaching noise markers on the face against deep face recognition. J. Inf. Secur. Appl. 60, 1–11. https://doi.org/10.1016/j.jisa.2021.102874.

Shao, Z., Zhang, L., Li, X., Guo, Y., 2019. Antecedents of trust and continuance intention in mobile payment platforms: the moderating effect of gender. Electron. Commer. Res. Appl. 33, 1–10. https://doi.org/10.1016/j.elerap.2018.100823.

Stewart, K.J., 2003. Trust transfer on the World Wide Web. Organ. Sci. 14, 5–17. https://doi.org/10.1287/orsc.14.1.5.12810.

Stewart, K.J., 2006. How hypertext links influence consumer perceptions to build and degrade trust online. J. Manag. Inf. Syst. 23, 183–210. https://doi.org/10.2753/MIS0742-1222230106.

Stone, M., 1974. Cross-validatory choice and assessment of statistical predictions. J. R. Stat. Soc. Ser. B 36, 111–133. https://doi.org/10.1111/j.2517-6161.1974.tb00994.x.

Tenenhaus, M., Vinzi, V.E., Chatelin, Y.-M., Lauro, C., 2005. PLS path modeling. Comput. Stat. Data Anal. 48, 159–205. https://doi.org/10.1016/j.csda.2004.03.005.

Turel, O., Yuan, Y., Connelly, C.E., 2008. In justice we trust: Predicting user acceptance of E-customer services. J. Manag. Inf. Syst. 24, 123–151. https://doi.org/10.2753/MIS0742-1222240405.

Vazquez-Fernandez, E., Gonzalez-Jimenez, D., 2016. Face recognition for authentication on mobile devices. Image Vis. Comput. 55, 31–33. https://doi.org/10.1016/j.imavis.2016.03.018.

Venkatesh, Morris, Davis, Davis, 2003. User acceptance of information technology: toward a unified view. MIS Q. 27, 425–478. https://doi.org/10.2307/30036540.

Venkatesh, T., Xu,, 2012. Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. MIS Q. 36, 157–178. https://doi.org/10.2307/41410412.

WeChat Pay, 2022. The introduction of frog. URL: https://pay.weixin.qq.com/wiki/doc/wxfacepay/product/ (accessed 4.12.22).

Williams, M.D., 2021. Social commerce and the mobile platform: Payment and security perceptions of potential users. Comput. Human Behav. 115, 105557 https://doi.org/10.1016/j.chb.2018.06.005.

Yang, Q., Pang, C., Liu, L., Yen, D.C., Michael Tarn, J., 2015. Exploring consumer perceived risk and trust for online payments: An empirical study in China's younger generation. Comput. Human Behav. 50, 9–24. https://doi.org/10.1016/j.chb.2015.03.058.

Yeung, D., Balebako, R., Gutierrez, C.I., Chaykowsky, M., 2020. Face Recognition Technologies: Designing Systems that Protect Privacy and Prevent Bias. RAND Corporation, Santa Monica, California.

Yuan, S., Liu, L., Su, B., Zhang, H., 2020. Determining the antecedents of mobile payment loyalty: Cognitive and affective perspectives. Electron. Commer. Res. Appl. 41, 1–9. https://doi.org/10.1016/j.elerap.2020.100971.

Zhang, K.Z.K., Gong, X., Chen, C., Zhao, S.J., Lee, M.K.O., 2019. Spillover effects from web to mobile payment services: the role of relevant schema and schematic fit. Internet Res. 29, 1213–1232. https://doi.org/10.1108/IntR-11-2017-0457.

Zhang, W.K., Kang, M.J., 2019. Factors affecting the use of facial-recognition payment: an example of Chinese consumers. IEEE Access 7, 154360–154374. https://doi.org/10.1109/ACCESS.2019.2927705.

Zhong, Y., Oh, S., Moon, H.C., 2021. Service transformation under industry 4.0: Investigating acceptance of facial recognition payment through an extended technology acceptance model. Technol. Soc. 64, 1–10. https://doi.org/10.1016/j.techsoc.2020.101515.

Zhou, T., 2011. An empirical examination of initial trust in mobile banking. Internet Res. 21, 527–540. https://doi.org/10.1108/10662241111176353.

Zhou, T., 2012. Understanding users ' initial trust in mobile banking : An elaboration likelihood perspective. Comput. Human Behav. 28, 1518–1525. https://doi.org/10.1016/j.chb.2012.03.021.