



# An Empirical Investigation of Intent to Adopt Mobile Payment Systems Using a Trust-based Extended Valence Framework

Amita Goyal Chin<sup>1</sup> · Mark A. Harris<sup>2</sup> · Robert Brookshire<sup>3</sup>

Accepted: 13 October 2020 / Published online: 3 November 2020  
© Springer Science+Business Media, LLC, part of Springer Nature 2020

## Abstract

The purpose of this research is to assess the impact of trust, when balanced with risk and benefit, on consumer intention to adopt mobile payment systems. A research model is created to assess intent based on perceived trust, along with three antecedents – privacy, security, and familiarity – and packaged with an extended valence framework that takes into account the opposing notions of perceived risk and perceived benefit. Following a pilot study of 76 participants, data is collected from a survey of 234 respondents and is analyzed using consistent Partial Least Squares (PLSc). Results indicate that perceived benefit and perceived trust are the most important influences on the intention to use mobile payment systems, and that the perceived risk of using mobile payment systems has little or no impact on intention to use. The risk result is explained by motivational avoidance theory and institutional dependence.

**Keywords** Mobile payment · Risk · Trust · Valence framework

## 1 Introduction

The ubiquitous penetration of mobile gadgets combined with the unequivocal advances in wireless communications have empowered a commonplace usage and commitment to mobile technology and consequently, a substantial boon to ecommerce, in particular, ecommerce facilitated by mobile devices, or mobile commerce (mcommerce). Mobile devices include smartphones, tablets, gaming consoles, fitness trackers, smart watches, smart rings, bracelets, personal digital

assistants (PDAs), and e-readers, (Chin et al. 2020; Harris and Patten 2014; Infineon n.d.; Jones 2018). Studies estimate some 3.9 billion smartphones were used globally in 2016, and this number will grow to 6.8 billion by 2022 (Ericsson 2017). Furthermore, with the availability of 5G in 2018, mobile data traffic, which is driven by both the rising number of smartphone subscriptions and the average data volume used per subscription, grew 54% in Q1 2018 with Q4 2018 witnessing a staggering addition of 43 million subscriptions (Jonsson et al. 2019). The various mobile apparatuses are not only used for entertainment, social exchanges, and academic pursuits, but have also become the predominant devices for executing business transactions (Chin et al. 2020; Jones and Chin 2015; Qasim and Abu-Shanab 2016), that is, for participating in mobile commerce. The two key devices that are propelling the mcommerce movement are smartphones and tablets (Meola 2019). Consumer engagement in shopping and purchasing using mobile devices, specifically feature-rich smartphones and tablets, is predicted to grow to \$488.0 billion, or 44% of ecommerce, in 2024 (Meola 2019). Therefore, mobile commerce, and in particular, the payment systems used to complete online and in-person transactions, have become important topics of investigation for both industry and academia (Gao et al. 2015).

A mobile payment is a regulated digital transaction that takes the form of a cashless, checkless, physical credit cardless payment made through a mobile device (Infineon n.d.). A

✉ Amita Goyal Chin  
agchin@vcu.edu

Mark A. Harris  
Mark.Harris@augusta.edu

Robert Brookshire  
rbrook@mailbox.sc.edu

<sup>1</sup> Department of Information Systems, School of Business, Virginia Commonwealth University, Room B4107 Snead Hall, 301 W. Main Street, Richmond, VA 23284-4000, USA

<sup>2</sup> School of Computer and Cyber Sciences, Augusta University Cyber Institute, 1120 15th Street, University Hall/UH- 127, Augusta, GA 30912, USA

<sup>3</sup> Integrated Information Technology, College of Engineering and Computing, University of South Carolina, Columbia, SC 29208, USA

mobile payment can be a credit card payment using a mobile wallet, where consumers can securely store the bank details associated with a debit card or one or more credit cards. Instead of using a physical credit card, which can be lost or stolen, credit card payment can be electronically made using the consumer's mobile device. A mobile payment can also occur when transferring money between individuals. For example, Venmo is very popular among college students because they can easily transfer money digitally to one another for a shared pizza or other purchases. Additional examples of popular mobile payment systems include Apple Pay, Google Pay, Samsung Pay, and PayPal (Viswanathan 2018). Mobile payments can occur in a variety of manners, such as paying at restaurants with a smartphone, using a smart watch or bracelet to pay at a vending machine, or transferring money to a friend without having to use cash (Jones 2018; Pinola 2018).

There are multiple technologies that mobile payment systems may use, such as near field communication (NFC) payments, magnetic security transmission (MST) payments, quick response (QR) code payments, and short message service (SMS) based payments (Sorensen 2018). NFC is a subset of radio frequency identification (RFID) that works with an NFC chip in the personal device and an NFC reader in the point-of-sale (POS) system (Cipriani 2015). MST works by sending encrypted data through a magnetic signal to the POS swipe card reader, essentially mimicking the swipe of a credit card (Cipriani 2015). MST and NFC are both currently available with Samsung Pay, but MST is not available on Apple Pay, Google Pay, or PayPal. Both NFC and MST need the personal device to be within a few inches of the POS in order to work, but devices do not need to touch the POS. QR payments work by scanning the merchant's bank-issued QR code with a personal device and entering the payment amount and personal identification number (PIN) (American Express n.d.). QR is gaining popularity because merchants only need to print their QR code and not invest in expensive technology (American Express n.d.). SMS based payments work by entering the correct information into a text message and sending it to a vendor specific number (Cipriani 2015). SMS payments began losing popularity as other technologies became more prevalent on smartphones (Cipriani 2015).

Consumers undergo an evaluation process, often subconsciously, when choosing a method of payment – cash, check, credit card, debit card, or mobile payment. Given the multitude of choices that are available to consumers, and the wide assortment of backend technologies powering the systems, each with varying security and privacy concerns, it has become of paramount importance to investigate the factors that sway consumers to adopt a mobile payment system. This decision may be based on a risk assessment of the technology (Kapoor et al. 2015), or a trust in the

vendor based on reputation (Harris and Chin 2016; Harris et al. 2015), or another factor such as a familiarity with the system or a perceived benefit of using the system.

The purpose of this research is to assess the impact of trust, when balanced with risk and benefit, on consumer intention to adopt mobile payment systems. Following a review of the published literature relating to mobile technology, a trust-based extended valence framework (EVF), adopted from Kim et al. (2009), is further enhanced to create a unique consumer decision-making model that incorporates privacy, security, and familiarity as antecedents to perceived trust and risk. Furthermore, in addition to considering trust as previously defined in the extant literature, this study extends previous work by incorporating motivational avoidance theory and institutional dependence (Shepherd and Kay 2012) from the psychology literature as a component of consumer trust in enigmatic circumstances, for example, when choosing to use a mobile payment system to complete a transaction. A new survey instrument is developed based on the multiple facets of trust as identified in previous works, balanced with both the assessment of risk and the perception thereof, and with the potential for benefit. Following a pilot study of 76 participants, data is collected from a survey of 234 respondents and is analyzed using consistent Partial Least Squares (PLSc). Finally, we present our results followed by a discussion on the research implications of our findings.

## 2 Previous Research

A review of the previous literature identified hundreds of publications relating to mobile payments, however, the majority of these prior works did not investigate mobile payment adoption. Three empirical studies recapitulated the previously published body of works. The first study reviewed 73 mobile payment manuscripts between 1999 and 2006 (Dahlberg et al. 2008). In the second, Dahlberg et al. (2015) continued with a follow-up summary of mobile payment research by investigating another 188 studies between 2007 and 2014. In both studies, the researchers did not focus on mobile payment adoption by consumers, but instead investigated multiple categories of mobile payment research, one of which was adoption. The first review found 14 adoption studies and concluded that these studies were dominated by models based on the Technology Acceptance Model (TAM), the Unified Theory of Acceptance and Use of Technology (UTAUT), and Diffusion of Innovation (DOI). In the second empirical review, the authors reviewed 34 adoption studies and determined that while researchers continued to rely on TAM, UTAUT, and DOI, they also started including Task-Technology Fit (TTF) theory, the Theory of Reasoned Action (TRA), and the Theory of Planned Behavior (TPB) (Dahlberg et al. 2015). The authors concluded that studies

after 2007 have failed to include innovative constructs and suggested that researchers introduce new theories beyond TAM and UTAUT for mobile payment adoption research (Dahlberg et al. 2015).

The third empirical review (Harris et al. 2019) of mobile payment studies identified 57 mobile payment adoption studies through 2018, 29 of which were published since 2014, the end of the second empirical review mentioned above. Harris et al. (2019) only included studies that used theoretical models and hypotheses to investigate mobile payment adoption. The most frequently employed theories across all years were TAM, UTAUT/UTAUT2, and DOI. The first two continued to be the recurrently used theories since 2014, again demonstrating the need for new theoretical models in investigating mobile payment adoption (Harris et al. 2019).

Our current research proposes the use of a trust-based extended valence framework, adopted from Kim et al. (2009), that includes trust, risk, benefit, and intention. The model is further enhanced with the antecedents of privacy, security, and familiarity. This model is further explained in the next section. Our literature review only found a few other mobile payment adoption studies that utilized a valence framework and none like ours. There were quite a few differences in these models, with most utilizing different theories and constructs, such as TAM, UTAUT, and DOI. One was a study by Lu et al. (2011), where they used DOI within the valence framework. They found significant relationships within the valence framework, with trust being more significant than risk. The researchers did not investigate benefit, privacy, security, or familiarity. Another valence framework mobile payment adoption study was from Ozturk et al. (2017), where that authors investigated negative and positive valence groups of constructs. Risk and privacy concerns were negative valence constructs and convenience and utilitarian value were positive valence constructs. The researchers also investigated individual differences. Results show significant relationships between intent and privacy concerns, convenience, and utilitarian value. However, the relationship between risk and intent was not significant, which is unusual. Another study from Yang et al. (2011) investigated a valence framework consisting of negative valence risk constructs and positive valence benefit constructs. This was not a risk/trust model and did not include privacy, security, or familiarity. There was a significant relationship between risk and intention. Another study that utilized the valence framework was from Guo and Waechter (2017). Their model was a TAM hybrid model that investigated initial trust and was not a risk/trust model. The researchers found a significant relationship between initial trust and perceived benefit.

A study by Park et al. (2019) did not introduce their model as a valence framework, but did contain the constructs risk, trust, benefit, and intention. The researchers did not investigate privacy, security, or familiarity, but instead

investigated moderating demographic variables gender, income, age, and education. All results were significant except benefit to intention, which was not significant. Cocosila and Trabelsi (2016) also did not list their model as a valence framework, but utilized constructs grouped as gain constructs and cost constructs. The researchers integrated perceived risk into perceived value. The model did not investigate trust, but it did find significant relationships between overall risk and integrated value risk and also between integrated value risk and intention. No valence framework study we found considered motivational avoidance or institutional dependence, as in our study.

We found other studies that investigated risk and trust in relation to the intention to adopt mobile payments. A study from Slade et al. (2015) found positive relationships between trust and risk, risk and intention, but not trust and intention. These findings contradict most research that includes trust. In another study, Khalilzadeh et al. (2017) investigated risk, trust, and security in an UTAUT model and found significant relationships between all three constructs and intention. Liébana-Cabanillas et al. (2014) used a TAM model to investigate risk and trust and found both had significant relationships with intention. A relationship between risk and trust was not tested. In other research from Liébana-Cabanillas et al. (2014), the researchers investigated risk and trust and found they have significant relationships between each other. Also, risk had a significant relationship with intention, but the relationship between trust and intention was not investigated.

Beyond the studies that used valence frameworks, we found other studies that used one or more of our antecedents of privacy, security, and familiarity. Familiarity was not found in any other mobile payment adoption study, but one study investigated similarity (Cao 2017). The authors defined similarity as “the degree to which mobile and PC-based online payments are perceived as similar in several dimensions, such as function and operation.” Our definition of perceived familiarity refers to “the consumer being comfortable with conducting transactions through a mobile payment system.” This implies the consumer is comfortable with dimensions such as function and operation and, thus, we see these constructs as analogous. In their study, perceived similarity was found to have a significant relationship with trust ( $p < .05$ ).

Privacy is not a common construct in mobile payment adoption research and is often seen as a component of risk and not often investigated with trust. In one study, Yang et al. (2011) investigated perceived privacy risk in relation to acceptance intention. Perceived privacy risk is a part of the uncertainty-risk-value framework and was found to have a significant relationship with acceptance intention. Security was not investigated. In another example, Morosan and DeFranco (2016) investigated privacy and

mobile payment adoption through two different constructs. Specific privacy measured a consumer's concern about their personal information while using NFC mobile payment and was found to have a significant relationship with intention. General privacy measured a consumer's general concern about their personal information and was found to not have a significant relationship with intention. In another study, Thakur (2014) investigated privacy risk as an antecedent of perceived risk and found it to be significant. The study did not investigate trust. Another study mentioned earlier that used a valence framework, but not trust, found that privacy risk had a significant relationship with intention (Ozturk et al. 2017).

The construct security was more abundant in studies than privacy and familiarity, but none were found that investigated security in a valence framework. Morosan and DeFranco (2016) investigated perceived security in relation to NFC specific privacy and intention. The relationship with NFC specific privacy was significant, but the relationship with intention was not significant. In another study, Thakur (2014) investigated perceived security and perceived risk and found the relationship between them to be significant. Zhou (2011) investigated perceived security and found it to have a significant relationship with trust. Trust was also found to have a significant relationship with intention. In addition, multiple other studies were found that demonstrated significant relationships between security and intention (Di Pietro et al. 2015; Aydin 2016; Oliveira et al. 2016; Liébana-Cabanillas et al. 2014; Yang and Lee 2016).

Overall, no study was found that utilized the trust/risk-based valence framework as we propose with the antecedents of familiarity, privacy, and security. We also found no studies in the information systems literature that considered motivational avoidance and institutional dependence as a component of trust. A few valence framework papers were found that investigated mobile payment adoption, but those frameworks utilized different theories, base-models, and antecedents. Most works included the construct of risk; all but one study found risk to have a significant relationship with intention (Ozturk et al. 2017). For our antecedents, the use of familiarity was not found, but an analogous use of similarity was found and had a significant relationship with trust. Privacy was mentioned in a few studies, but most studies did not investigate privacy. In general, privacy was found to have significant relationships with perceived risk and intention. Security was found in more studies than familiarity and privacy and typically had significant relationships with perceived risk and intention. Based on our literature review, we believe that our proposed model fits the statement from Dahlberg et al. (2015) in their call for new research that utilizes new theoretical ways to investigate mobile payment adoption.

### 3 Theoretical Background

The explosive saturation and subsequent omnipresence of mobile technology, or mTechnology as coined in (Chin et al. 2018), amalgamated with the tremendous burgeoning of utilitarian mobile apps, or mApps, that ease and expedite the performance of routine tasks and provide ready access to entertainment has entrenched a prodigious customer base. New retail channels, which are often devoid of a traditional brick-and-mortar presence, have necessitated a need for mobile payments in lieu of physical payment mediums, such as cash or cards, combined with geographic proximity. The massive proliferation of mobile phones has resulted in these devices serving as ideal conduits and enablers of mobile payment systems (Chin et al. 2020). For example, mobile phones can be used to send an SMS to execute a mobile payment and have the charge appear on a customer's phone bill (Menke and de Lussanet 2006) or can be used to execute an electronic payment using traditional means such as a bank account or a debit or credit card (Mallat 2007).

While disclosing personal information using this new medium for payment can be disconcerting to consumers and may serve as somewhat of a deterrent for engagement (Dinev and Hart 2006; Groß 2016), eCommerce sales have continued to rise. Consumers are cognizant, at least at some conscious level, of the plethora of risks that are a component of eCommerce but realize that they cannot anticipate and mitigate all of these risks (Groß 2016). A calculus of a cumulative antecedent to information disclosure, where the consumer must balance multiple criteria including perceived risk, institutional norm, personal beliefs and trust, with anticipated benefit, to then settle on a paradoxical choice has been identified in previous works (Dinev and Hart 2006; Culnan and Armstrong 1999; Laufer and Wolfe 1977). The extant literature includes numerous studies focused on predicting human behavior, particularly in the context of a trust-risk relationship (Gu et al. 2016; Hassoy et al. 2013; Hillman and Neustaedtler 2016; Qiu et al. 2013; Yan et al. 2013). Consumers choose to participate in eCommerce, facilitated by mobile payments, intrinsically assuming some level of institutional dependence and subsequent personal protection, as mobile payments provide numerous benefits including expediency in purchasing.

In the present research, our theoretical model draws from the theory of reasoned action to understand user tendencies to adopt mobile payment systems. Furthermore, we apply the theory of motivated avoidance of sociopolitical information to better explain the results of the theoretical model. We contribute to the established body of knowledge by evaluating the impact of trust – with the antecedents of privacy, security, and familiarity – balanced with risk and benefit as antecedents to consumer intent to adopt mobile payment systems.

The theory of reasoned action (TRA) (Fishbein and Ajzen 1975) posits that behavioral intentions are the immediate



antecedents to actual behavior and are influenced by beliefs about the likelihood that performing a particular behavior will lead to a specific outcome (Madden et al. 1992). That is, the TRA addresses the relationship between an individual’s attitudes, subjective norms, and perceived behavioral control as constructs that influence intentions. At its core, the theory assumes that human beings are rational and make rational choices based on the information that they have available to them. The TRA suggests that the best immediate determinant of a person’s actual behavior is the person’s intent, which is the cognitive representation of readiness to perform a given behavior (Ajzen and Fishbein 1980). The theory of planned behavior (TPB) (Ajzen 1991), an extension to the TRA, has been extensively utilized in the literature to model intentions to engage in a behavior and to study intentions in order to predict behavior under various scenarios.

Relying on the TRA as the theoretical foundation, Kim et al. (2009) developed the extended valence framework (EVF), a risk- and trust-based consumer decision-making model, as shown in Fig. 1. The EVF integrates the TRA-based trust building model (TBM) (McKnight et al. 2002) and the valence framework (Goodwin 1996) to explain purchase intention, in particular as it pertains to eCommerce, as an immediate precursor to actual purchase behavior.

The TBM posits that trusting beliefs (in the competence, benevolence, and integrity of the vendor) lead to trusting intentions (making oneself vulnerable to the vendor), which in turn influence trust-related behaviors (McKnight et al. 2002). That is, trust is a direct precursor to intention. The valence framework, derived primarily from the economics and psychology literature, has been used by game theorists and market researchers to understand behaviors that incorporate the simultaneous perception of risk and benefit (Peter and Tarpey 1975). Perceived risk and perceived benefit are fundamental aspects of consumer decision-making. In this dichotomous relationship, consumers are motivated to minimize the negative facets of risk while maximizing the positive facets of benefit. This yields a perceived value from the activity, or net valence, which is computed as the difference of the attributes of risk and the attributes of benefit.

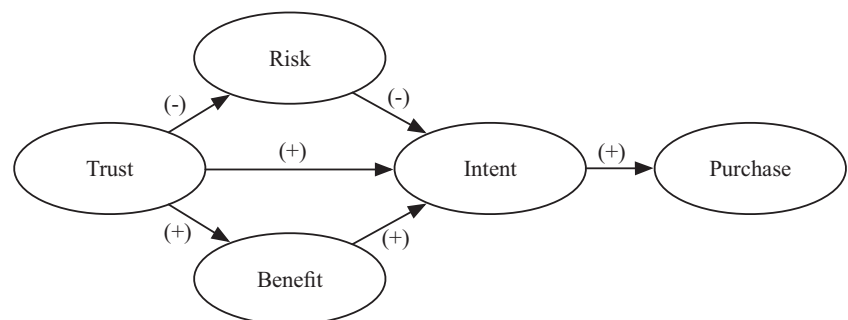
To better understand the results of the theoretical model, we turn to Shepherd and Kay (2012) and their theory of

motivated avoidance of sociopolitical information, which is based on system justification theory (Jost and Banaji 1994) and the subsequent compensatory control theory (Kay et al. 2008). Shepherd and Kay (2012), invoking cognitive dissonance theory, argue that “to the extent that people increasingly trust or justify the legitimacy of an authority to cope with their dependence on it, they should be motivated to avoid information that could potentially rupture this trust” (Shepherd and Kay 2012).

Using three distinct hypothetical scenarios, Shephard and Kay (2012) show that when feeling overwhelmed and unknowledgeable about significantly alien subject matter, rather than foraging for additional information, consumers are likely to increase their dependence on the institutional authority governing a system, which in turn increases their level of trust in the systems that they are using and in the institution (McKnight et al. 2002; Suh and Han 2003; Kim and Prabhakar 2004). Furthermore, given this established trust, consumers inherently resist any new data that could weaken their trust in the institution, and they actively avoid new information about complex topics. Our increasing dependence on device manufacturers, software vendors and government agencies to guarantee our security leads us from dependence on these entities to a psychological acceptance of blind trust in these entities and a convenient relinquishment and a motivated avoidance of individual duty for ensuring safety when issuing a mobile payment (Chin et al. 2016).

The theory of motivated avoidance was operationalized in Chin et al. (2018) to explain user acquiescence when downloading mApps. However, it has never previously been applied to mobile payment systems, and in particular, to the intent of consumers to participate in a mobile payment system. The theoretical propositions of motivational avoidance can be used to rationalize the psychological inclinations of complacency toward security when originating a mobile payment transaction. The Shepherd and Kay (2012) model describes a behavioral path beginning with a “psychological discomfort associated with epistemic uncertainty.” With the myriad of options now available for mobile payments, including for example, Apple Pay, Google Pay, Samsung Pay and PayPal, and the multitude of vendors that are readily equipped to accept such payments, submitting an electronic transfer of

**Fig. 1** Extended Valence Framework (EVF) from Kim et al. (2009)



funds has come in vogue and its efficiency incontrovertible in spite of the fact that the technical aspects and the intricate web of processes that must transpire when utilizing a mobile payment remains a source of perplexity and uncertainty for most individuals (Chin et al. 2018). Individually mastering and disentangling the multifarious issues associated with securing one's mobile payments is a complex and arguably insurmountable activity, and the associated anxiety from the inability to decipher and process information particulars leads individuals to "simply outsource personal responsibility to supposed qualified others" (Shepherd and Kay 2012). The dominating desire and expectation for the resulting benefit – an increase in personal productivity or personal pleasure – then prevails over the notions of perceived risk in favor of an implicit assumption of institutional dependence.

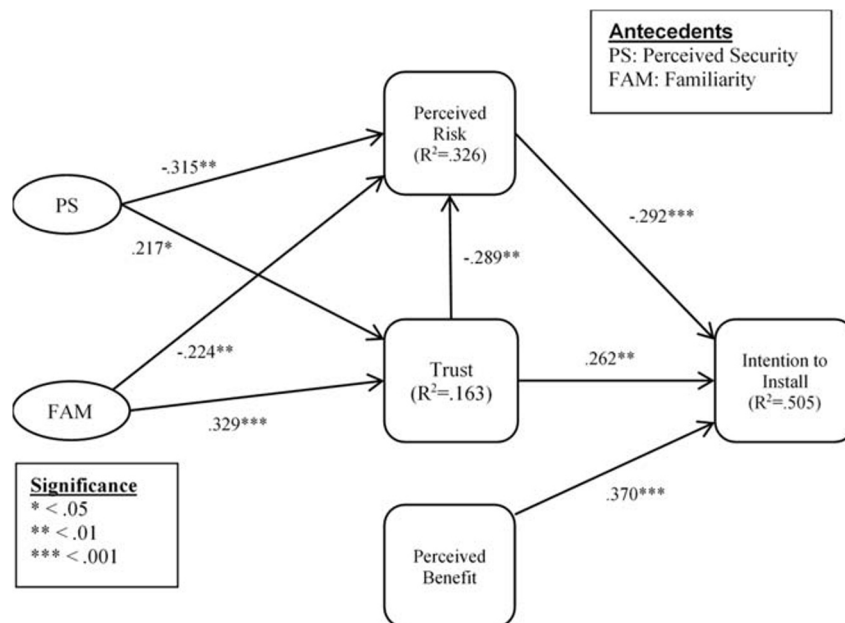
Trust is a key underlying element of any transactional activity, where trust can be broadly defined as "the willingness of one party (trustor) to depend or rely on the actions of another party (trustee) (Bisdikian et al. 2014)." Users are unable to establish indisputable and absolute trust when processing a mobile payment but are unwilling to succumb to the fears of risk and uncertainty to the extent of disengaging from an online transaction, and therefore, are willing to accept dependence on institutions, institutional norms and processes for their safety. That is, it becomes reasonable to trust the device manufacturers and software companies to fortify our devices and safeguard us against risk, in effect tempering our need for security awareness and actual security behavior. For example, users rely on the seller feedback rating on eBay, and they are more likely to purchase an item, especially a large ticket item, from a seller with a high number of positive ratings rather than from a seller with low feedback or consistent negative ratings

(Masclet 2012; Yan et al. 2012). Individuals are unable to personally investigate each seller, and therefore, delegate the establishment of trust to eBay, creating a personal dependence on this institution and its filtering protocols. Similarly, in issuing a mobile payment, consumers place their trust in established eTailers including Apple, Google, and PayPal, for example. In so doing, the fears of the potential invasion of personal privacy, the resulting threats to security, and other possible negative ramifications resulting from generating a mobile payment are relegated to obscurity in favor of a reliance on trust in these institutions.

## 4 Research Model and Hypotheses

We base our research model to assess the impact of trust on the intent to adopt mobile payment systems on multiple related models previously published in the recent literature. Harris et al. (2016) developed a research model to evaluate several antecedents to trust when investigating consumer intention to install mobile applications, including perceived security, perceived reputation, familiarity, and desensitization (see Fig. 2). They concluded that only perceived security and familiarity were significant to perceived risk and perceived trust. While perceived benefit was included in their model, it was not linked to perceived trust. Chin et al. (2018) extended Trust-to-Risk and Risk-to-Trust unidirectional models from Kim and Koo (2016) to construct a bidirectional model between trust and risk as indicators of intention to install mobile applications (see Fig. 3). In this model, privacy was independently evaluated as an antecedent to risk while security was independently evaluated as an antecedent to trust. Risk and trust were

**Fig. 2** Reduced research model from Harris et al. (2016)



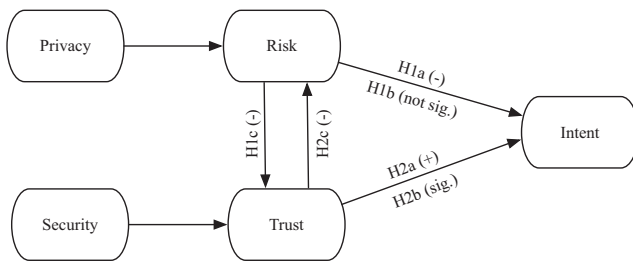


Fig. 3 Bidirectional research model from Chin et al. (2018)

hypothesized to have a significantly negative relationship with each another, however, this was not supported by their data. The effect of perceived benefit was not considered in this model.

Kim et al. (2009) proposed an Extended Valence Framework (EVF) which incorporates both risk and benefit into the research model (see Fig. 1), and valence is the subjective value, attachment or preference that each individual attributes to a reward. The valence framework stemming from economics and psychology literature (Goodwin 1996) has been used to better understand the decision-making process where the perception of risk is offset with the expectation of benefit (Kim et al. 2009). That is, consumers are motivated to engage in transactions that minimize risk of loss or failure and at the same time, are motivated to accept actions that will maximize potential gain or benefit. Peter and Tarpey (1975) consider perceived risk/cost and perceived benefit as two fundamental aspects of decision-making. Risks and costs are defined as a seller’s belief about the potential uncertain negative outcomes from an online transaction. Benefits are defined as a seller’s belief about the extent to which the seller will become better off from an online transaction through a certain website. According to the theory, a net positive valence, i.e. a situation where benefits exceed the costs, should result in a higher positive behavioral intention. In the context of the intent to use a mobile payment system, valence is computed as the difference between the perceived risk in engaging in a mobile payment transaction – for example, loss of privacy – and the perceived benefit – for example, the convenience – of such participation. If the risk outweighs the benefit, the valence is negative whereas benefit prevailing over risk results in a positive valence. Given this simultaneous tug-of-war of positive versus negative, the valence framework assumes consumers will opt to maximize the net valence in an action (Kim et al. 2009; Peter and Tarpey 1975).

In developing our research model, we logically coalesce these previously published frameworks to facilitate a robust examination of consumer intention to purchase online goods/services and extend them to investigate consumer intent to adopt mobile payment systems. The reduced, refined model in Harris et al. (2016) included two antecedents to perceived risk, namely, perceived security and familiarity. The authors elected to include both security and privacy as components of

their security antecedent rather than creating two distinct antecedents to represent these important factors. While combining privacy and security is commonplace in the research literature (Harris et al. 2016; Amoroso and Magnier-Watanabe 2012; Schierz et al. 2010; Mallat 2007; Albashrawi and Motiwalla 2019), we believe that privacy and security should be modeled as two distinguishable antecedents in order to garner a better understanding of their unique relationship with trust and risk. This notion is consistent with multiple previous works that have separated privacy and security into two distinct terms (Sicari et al. 2015; Pearson 2013; Chin et al. 2012; Bélanger et al. 2002; Ismagilova et al. 2020). Next, we extend the model in Chin et al. (2018), where privacy is considered only as an antecedent to risk with no direct relation to trust, to serve as an antecedent to both risk and trust. While Kim et al. (2009) propose the EVF to show consumer decision making as it pertains to executing purchases in the online space, we employ EVF in two different ways. First, we investigate factors that input into the EVF. That is, as a logical precursor to evaluating consumer decision-making based on the net valence of risk and benefit as indicators of intent, we position the three antecedents of privacy, security, and familiarity as factors that influence trust. Second, we capture the paradoxical relationship between risk and benefit using the EVF in the context of consumer decision making to adopt mobile payment systems. All constructs, antecedents, and related hypotheses of our research model are detailed in Fig. 4.

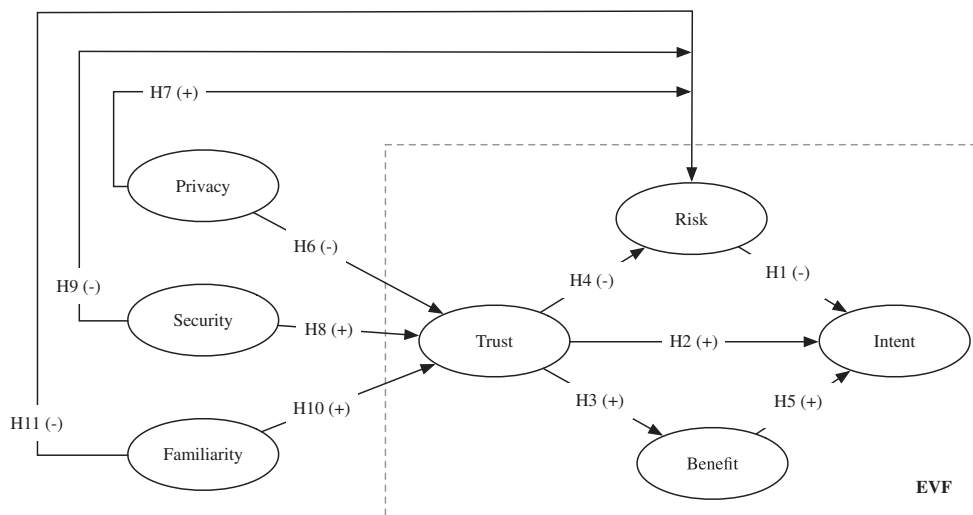
### 4.1 Intention to Use

Previous theoretical research has demonstrated that a consumer’s intention is a significant predictor of their actual behavior (Taylor and Todd 1995; Venkatesh et al. 2003; Pavlou 2003; Kim et al. 2008; Shin 2009; Yang 2013). In mobile payment adoption research, Shin (2010) found that the intention to adopt a mobile payment system had a significant relationship with actual adoption. Therefore, in our research, a consumer’s intention to adopt a mobile payment system is seen as a significant predictor of their actual adoption of such a system.

### 4.2 Perceived Risk

Researchers have identified many different variants of risk. For example, Jacoby and Kaplan (1972) identified seven types of risks: financial, performance, physical, psychological, social, time, and opportunity cost risk. Kim et al. (2008) identified information risk as associated with transaction security and privacy. In studying the adoption of a mobile payment system, perceived risk is best aligned with financial risk and information risk, where perceived risk is defined as a consumer’s “subjective expectation of suffering a loss in pursuit of a desired outcome (Warkentin et al. 2002).” Pavlou (2003)

Fig. 4 Research model



and Kim et al. (2008) found that perceived risk had a negative effect on the intention to conduct ecommerce transactions. However, Wu and Wang (2005) found that perceived risk had a significantly positive effect on the intention to use certain services, including for example, eGovernment services (Bélanger and Carter 2005). Looking more specifically at mobile payment adoption research, Shin (2010) used a hybrid of the Technology Acceptance Model (Davis 1989) and found that perceived risk had a significant negative relationship with intention. In other mobile payment adoption research, Lu et al. (2011) also found that perceived risk had a significant negative relationship with intention. In research investigating mobile application installation and online purchases, researchers discovered significant negative relationships between perceived risk and intent Harris et al. 2016; Kim et al. 2008; Pavlov and Gefen 2004). Thus, we propose (see Fig. 4) that:

**Hypothesis 1** A consumer's perceived risk negatively affects a consumer's intention to use mobile payment systems.

#### 4.3 Perceived Trust

When using mobile payment systems to make purchases and transfer money, there is a level of risk that the consumer must consider, such as losing their personal funds. To combat risk, a consumer may rely on trust in the merchant. For example, an inverse relationship is expected where a consumer may perceive less risk if they have increased trust, such as performing transactions through a trusted provider. The more a consumer trusts their mobile payment platform, the less risk they will perceive, and the more intent they will have to adopt the platform. These relationships have been demonstrated in multiple studies in mobile payment adoption, where results have shown that trust had a significant positive relationship with the intention to adopt mobile payment systems (Shin 2009, 2010; Matemba et al. 2018). It has also been shown that trust

has a significant negative relationship with perceived risk (Khalilzadeh et al. 2017; Slade et al. 2015; Liebana-Cabanillas et al. 2014). In the EVF, Kim et al. (2009) assume that in addition to directly effecting the intention to make an online purchase, trust indirectly effects intent through its two mediators, perceived risk and perceived benefit.

The benefit a consumer receives from adopting a mobile payment system can come in various forms. The relationship between trust and benefit is rarely researched (Kim et al. 2009). Kim et al. (2009) argue that consumers can receive benefits from using trusted services, such as cost savings, time savings, convenience, and ease of use. Gao and Waechter (2017) and Kim et al. (2009) investigated this relationship and found the relationship was significantly positive. Therefore, we propose the following hypotheses (see Fig. 4):

**Hypothesis 2** A consumer's perceived trust positively affects the consumer's intention to use Mobile Payment Systems.

**Hypothesis 3** A consumer's perceived trust positively affects the consumer's perceived benefit of Mobile Payment Systems.

**Hypothesis 4** A consumer's perceived trust negatively affects the consumer's perceived risk of Mobile Payment Systems.

#### 4.4 Perceived Benefit

Perceived benefit is defined as the extent to which a consumer believes he or she will benefit from adopting a mobile payment system. Potential consumer benefits of using mobile payment systems may include cost savings, time savings, and convenience. Benefit in the valence framework works in contrast with perceived risk. While perceived risk discourages online activity, perceived benefit encourages consumers to engage in online transactions. Consumers perceive both



negative and positive attributes in making a decision (Kim, Ferrin, and Rao 2008). As perceived benefit increases, it is expected that the intent to adopt will increase.

De Kerviler et al. (2016) investigated this relationship and the results indicate a positive significant relationship. In other research, Harris et al. (2016) investigated factors that impact the installation of mobile apps and found that benefit had a significant positive relationship with intent to install. In online purchasing research, Kim et al. (2008) also found a significant positive relationship. Accordingly, we propose the following hypothesis (see Fig. 4):

**Hypothesis 5** A consumer's perceived benefit positively affects a consumer's intention to use mobile payment systems.

#### 4.5 Perceived Privacy

A consumer may be worried that mobile payment systems will collect and share their personal information with other entities (Keith et al. 2015), violating their privacy. The lack of privacy and security in online transactions, including the breach of personal data and the insecure transfer of financial data, continues to hinder the adoption of ecommerce (Quelch and Klein 1996; Aldás-Manzano et al. 2009). In our research, we expect that as privacy concerns increase, perceived trust will decrease and perceived risk will increase. Contrarily, as perceived privacy concerns decrease, perceived trust will increase and perceived risk will decrease.

No prior mobile payment adoption studies were found that measured the influence of perceived privacy concern on perceived risk or trust. However, other research has demonstrated that as privacy concerns decrease, perceived trust increases and perceived risk decreases. (Aloudat et al. 2014; Currás-Pérez et al. 2013; Kim et al. 2008). Therefore, we posit (see Fig. 4) that:

**Hypothesis 6** A consumer's perceived privacy concern negatively affects the consumer's perceived trust of mobile payment systems.

**Hypothesis 7** A consumer's perceived privacy concern positively affects the consumer's perceived risk of mobile payment systems.

#### 4.6 Perceived Security

Perceived security is “the subjective probability with which consumers believe that their personal information will not be viewed, stored, and manipulated during transit and storage by inappropriate parties in a manner consistent with their confident expectations” (Flavian et al. 2006). Even more important than the actual security measures that are in place is the consumer's own perceptions of achieved security that mainly

influences trust and intention (Chellappa and Pavlou 2002). Given that successful electronic transactions require the sharing of personal and financial information, concerns over the security of this information and its protection from unauthorized interception and fraudulent use have become paramount, especially in light of the recent data security breaches from compromised corporate systems, including that of Target and Home Depot. A consumer's perceived security refers to their perception that the mobile payment system will provide secure transactions. For example, consumers want to know their financial accounts are secure, data is protected, and payments go to the correct parties for the correct amounts. It is expected that as perceived security increases, trust will increase and risk will decrease.

In mobile payment research, several researchers have found that perceived security had a significant positive relationship with trust (Khalilzadeh et al. 2017). However, most mobile payment adoption research used TAM and UTAUT/UTAUT2 models, so no studies were found that investigated perceived security and perceived risk. In other research, perceived security was found to have a positive relationship with trust and a negative relationship with risk (Harris et al. 2016; Kim et al. 2008). Thus, we propose the following hypotheses:

**Hypothesis 8** A consumer's perceived security positively affects the consumer's perceived trust of Mobile Payment Systems.

**Hypotheses 9** A consumer's perceived security negatively affects the consumer's perceived risk of Mobile Payment Systems.

#### 4.7 Perceived Familiarity

Alba and Hutchinson (1987, p. 411) define familiarity as “the number of product-related experiences that have been accumulated by the consumer.” In the context of ecommerce, a consumer's perceived familiarity refers to the consumer being comfortable with conducting transactions through a mobile payment system. Consumers that are successful and satisfied with this process are likely to engage in the process again. The more familiar consumers are with the successful process, the more they expect the vendors to continue to honor their obligations; thus, consumers may feel more comfortable with the overall process (Kim et al. 2008; Harris et al. 2016) and, thus have an increased perception of trust and a reduced perception of risk.

Previous research literature has studied familiarity in the context of consumer behavior, where it has been shown that familiarity affects consumer decision making and is thus a central construct with which to explain consumer choices (Park and Lessing 1981; Johnson and Russo 1984; Rao and Monroe 1988). Several prior studies have examined the

effects of familiarity on consumer behavior and intentions (Coupey et al. 1998; Arora and Stoner 1996). Previous research has found that familiarity has a positive relationship with perceived trust (Gefen 2000) and a negative relationship with perceived risk (Kim et al. 2008; Harris et al. 2016; Miyazaki and Fernandez 2001). Thus, we posit the below hypotheses (see Fig. 4):

**Hypothesis 10** A consumer’s perceived familiarity positively affects the consumer’s perceived trust of Mobile Payment Systems.

**Hypothesis 11** A consumer’s perceived familiarity negatively affects the consumer’s perceived risk of Mobile Payment Systems.

## 5 Data Collection

A survey questionnaire was used to collect data. The survey was administered online using Qualtrics and was designed to measure the antecedent predispositions of consumers, including their perception of the security of mobile payment systems, their perception of the degree to which the system will protect their privacy, and their familiarity with mobile payment systems. The survey assessed their perception of risk involved in using mobile payment systems as well as their trust in the systems. In addition, user perceptions of the benefits of using the system was measured, along with their intention to use mobile payment systems. Finally, the survey collected basic demographic information.

Measurement scales from previous research were adapted for the present study. In particular, the measures of perceived security and perceived privacy were adapted from similar measures used by Kim et al. (2008). The measures of familiarity were adapted from Gefen (2000). Perceived risk measures were adapted from Pavlou and Gefen (2004). The indicators of trust were adapted from Pavlou and Gefen (2004) and Nicolaou and McKnight (2006). Indicators of benefit were adapted from Kim et al. (2008), along with new items constructed for this study. Measures of intention to use were adapted from Kim et al. (2008) and Pavlou and Gefen (2004). All attitude items were measured with a seven-point Likert scale ranging from “strongly disagree” to “strongly agree.” Appendix contains details on the questions used to measure the constructs as well as descriptive statistics for the measures.

Prior to administering the formal survey, a pilot study was conducted using the online survey instrument with 76 information technology students at a large southeastern research university. The resulting construct reliabilities as measured by Cronbach’s alpha were all greater than 0.70; therefore, no changes to the measurement items were made.

Following the pilot study, invitations to participate in this research study were sent by email to students enrolled in business technology classes at two large public research universities in the southeastern United States. The invitations were sent by the instructors of the classes. Several rounds of invitations were sent during the academic semester. The final number of students who agreed to participate was 234.

As shown in Tables 1 and 62.4% of the respondents were male and 37.6% were female. The ages of the participants ranged from 18 to 66, with a mean of 22.38, which is consistent with the survey being administered to college students. While 50% of the respondents identified their ethnicity as “white, not Hispanic,” 22% indicated they were African American, 13% were Asian, 5% were Hispanic or Latino, and 9% were of other ethnicities; 1% of the respondents preferred not to specify their ethnicity. The majority of the respondents were undergraduate students enrolled in a business major, including information systems.

## 6 Results

The construct reliability of the measures was evaluated first by examining the convergent validity of the measurement items. As shown in Table 2, all of the item loadings are greater than 0.708, indicating adequate shared variance between the items and their constructs (Hair, et al. 2019). Reliability measures for the latent variables in the model are shown in Table 3. Values for Chronbach’s alpha all exceed 0.70 and range from 0.828 to 0.919. Composite reliabilities all exceed 0.80 and range from 0.826 to 0.920. Likewise, all measures of the average variance extracted (AVE) are greater than 0.50, ranging from 0.617 to 0.850.

The discriminant reliability of the measures was evaluated by examining the loadings of the indicators on their constructs compared to their loadings on other constructs. As seen in Table 3, all indicators loaded at or above the cutoff value of 0.70, and the loadings of each indicator on its construct were well above 0.10 higher than their loadings on other constructs.

**Table 1** Respondent demographics

Gender	n	%
Male	146	62.4
Female	88	37.6
Ethnicity		
White	117	50.0
African American	52	22.2
Asian	31	13.2
Hispanic	11	4.7
Other	20	8.5
Not specified	3	1.3

**Table 2** Item loadings and reliability measures

Construct	Item	Standardized Loading	Cronbach’s Alpha	Composite Reliability	AVE
1. Perceived Security	1.1	0.806	0.891	0.899	0.730
	1.2	0.804			
	1.3	0.946			
2. Perceived Privacy	2.1	0.920	0.883	0.880	0.711
	2.2	0.816			
	2.3	0.788			
3. Familiarity	3.1	0.923	0.909	0.909	0.770
	3.2	0.867			
	3.3	0.839			
4. Perception of Risk	4.1	0.893	0.899	0.900	0.750
	4.2	0.797			
	4.3	0.905			
5. Perception of Trust	5.1	0.920	0.828	0.826	0.617
	5.2	0.705			
	5.3	0.712			
6. Perception of Benefit	6.1	0.870	0.919	0.920	0.793
	6.2	0.858			
	6.3	0.941			
7. Intention to Use	7.1	0.917	0.955	0.955	0.877
	7.2	0.927			

**Table 3** Measurement item crossloadings

Indicator	Perceived Security	Perceived Privacy	Familiarity	Perception of Risk	Perception of Trust	Perception of Benefit	Intention to Use
1.1	<b>0.806</b>	-0.104	0.204	-0.228	0.527	0.429	0.431
1.2	<b>0.804</b>	-0.045	0.194	-0.189	0.541	0.371	0.467
1.3	<b>0.946</b>	-0.185	0.287	-0.246	0.627	0.535	0.722
2.1	-0.128	<b>0.920</b>	-0.039	0.403	-0.272	-0.144	-0.125
2.2	-0.099	<b>0.816</b>	-0.135	0.334	-0.274	-0.205	-0.149
2.3	-0.113	<b>0.788</b>	-0.116	0.324	-0.263	-0.167	-0.124
3.1	0.296	-0.148	<b>0.923</b>	-0.074	0.359	0.408	0.532
3.2	0.226	-0.082	<b>0.867</b>	-0.008	0.344	0.406	0.509
3.3	0.184	-0.059	<b>0.839</b>	-0.037	0.33	0.340	0.442
4.1	-0.216	0.393	-0.082	<b>0.893</b>	-0.171	-0.004	-0.145
4.2	-0.212	0.330	-0.006	<b>0.797</b>	-0.142	-0.076	-0.133
4.3	-0.246	0.369	-0.029	<b>0.905</b>	-0.155	-0.028	-0.155
5.1	0.647	-0.275	0.356	-0.212	<b>0.920</b>	0.413	0.567
5.2	0.429	-0.261	0.295	-0.055	<b>0.705</b>	0.384	0.444
5.3	0.463	-0.217	0.268	-0.139	<b>0.712</b>	0.401	0.414
6.1	0.454	-0.173	0.351	-0.035	0.463	<b>0.870</b>	0.537
6.2	0.459	-0.192	0.402	-0.049	0.429	<b>0.858</b>	0.550
6.3	0.489	-0.176	0.419	-0.024	0.459	<b>0.941</b>	0.612
7.1	0.590	-0.155	0.518	-0.126	0.545	0.600	<b>0.917</b>
7.2	0.593	-0.134	0.523	-0.181	0.581	0.574	<b>0.927</b>

The heterotrait-monotrait matrix was also used to evaluate the discriminant validity of the indicators. As shown in Table 4, all the values are well less than 0.85 (Henseler et al. 2014), indicating adequate discriminant validity. Common method bias was examined with Harman's single factor test (Harman 1976; Podsakoff et al. 2003), which indicated that a single factor accounted for less than 35% of the total variance of the measures.

The model was estimated with consistent partial least squares (Dijkstra and Henseler 2015) using SmartPLS 3.2.7 (Ringle et al. 2015). Bootstrapping was used to calculate confidence intervals. See Park et al. (2019) for a succinct discussion of the use of partial least squares in information systems research. The structural model was evaluated by examining the direction and significance of the hypothesized relationships as described in the previous section.

The results of the hypothesis testing are shown in Fig. 5 and summarized in Tables 5, 6 and 7.  $R^2$  values indicate moderate to strong explanatory power of the endogenous variables, and the values of  $Q^2$  are mostly consistent with the values of  $R^2$  (Hair et al. 2019). In particular, the  $Q^2$  value for intention to use mobile payments was the largest of all endogenous variables. Our research model accounted for some variability in the respondents' perceived risk (adjusted  $R^2 = 0.233$ ) and their perception of benefit (adjusted  $R^2 = 0.256$ ) from mobile banking systems. In addition, our model accounted for substantial variability in perceived trust (adjusted  $R^2 = 0.536$ ) and the intention to use these systems (adjusted  $R^2 = 0.524$ ).

Looking at the path coefficient statistics in Table 6, the  $f^2$  values of  $f^2$  are consistent with the  $t$  values, and the variance inflation factor values are all below 3.0, indicating little threat to the results from collinearity (Hair et al. 2019).

Hypothesis 1 was not supported; although the relationship was in the predicted direction, it was not statistically significant ( $t = 1.516$ ,  $p = .130$ ). Hypothesis 2 was supported, as the consumers' perceived trust positively

affects their intention to use mobile payment systems ( $t = 4.801$ ,  $p < .001$ ). Hypothesis 3 was supported, as perceived trust positively affects perceived benefit ( $t = 9.164$ ,  $p < .001$ ). Hypothesis 4 was not supported, as the predicted relationship between perceived trust and perceived risk was not statistically significant ( $t = 1.110$ ,  $p = .268$ ).

Hypothesis 5 was supported — perceived benefit positively impacts the consumers' intention to use mobile payment systems ( $t = 6.645$ ,  $p < .001$ ). Likewise, hypothesis 6 was supported, as consumers' privacy concerns negatively affect their perceived trust in mobile payment systems ( $t = 3.015$ ,  $p = .003$ ). Hypothesis 7 was also supported, as their privacy concerns positively influence their perception of risk in these systems ( $t = 5.903$ ,  $p < .001$ ).

Our analysis found evidence to support hypothesis 8, that consumers' perceived security positively affects their perceived trust in mobile payment systems ( $t = 9.651$ ,  $p < .001$ ). Likewise, their perception of the security of these systems negatively affects their perception of risk when using them, supporting hypothesis 9 ( $t = 2.747$ ,  $p = .006$ ). Hypothesis 10 was supported, as consumers' familiarity with mobile payment systems positively affected their perceptions of trust in those systems ( $t = 3.218$ ,  $p = .001$ ). However, we did not find evidence to support hypothesis 11, that their familiarity with mobile banking systems negatively affected their perception of risk when using them ( $t = 0.306$ ,  $p = .760$ ).

## 7 Discussion and Conclusion

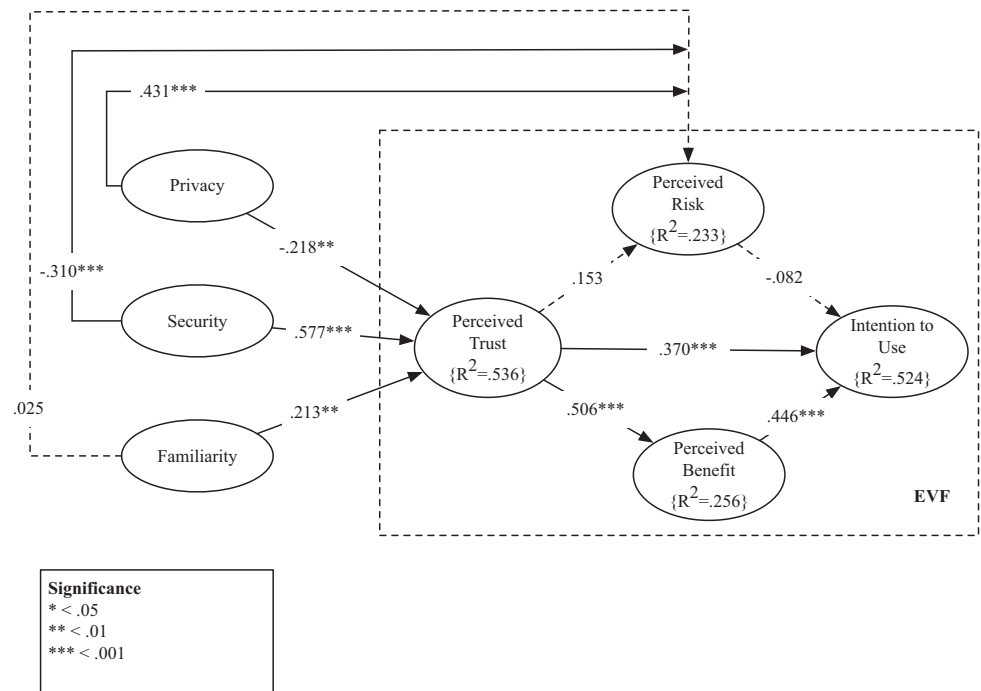
The rapid growth of eCommerce, fueled by the unequivocal growth of mTechnology, and including the recent surge in mobile payment systems that further enable eCommerce transactions, has focused concern on issues of privacy, trust, and personal risk. Prior empirical studies (Jones et al. 2014; Jing et al. 2014; Jorgensen et al. 2015) indicate that consumers are apprehensive about relinquishing personal and financial information in order

**Table 4** Heterotrait-monotrait (HTMT) matrix

Construct	Perceived Security	Perceived Privacy	Familiarity	Perception of Risk	Perception of Trust	Perception of Benefit	Intention to Use
Perceived Security							
Perceived Privacy	0.142						
Familiarity	0.290	0.117					
Perception of Risk	0.268	0.395	0.057				
Perception of Trust	0.658	0.311	0.391	0.173			
Perception of Benefit	0.530	0.205	0.428	0.045	0.495		
Intention to Use	0.677	0.142	0.574	0.169	0.610	0.636	



Fig. 5 PLS-SEM results



to engage in mobile transactions. While the popularity of mobile payment has been increasing worldwide, the adoption rates in the United States and Canada are relatively low. The United States’ adoption rate is 17%, Canada is 14%, but Mexico is 38% (Inscoe 2017). The Asia-Pacific region has higher adoption rates, including 56% in India and 51% in Thailand (Inscoe 2017). Europe, the Middle East, and Africa also have higher rates of adoption. For example, Spain has a 25% adoption rate, Italy 24%, UAE 38%, and South Africa 23% (Inscoe 2017). Inscoe (2017) reports that adoption rates are higher in countries that lack other electronic payment options, such as credit cards. In contrast, adoption rates are lower in countries, like the U.S. and Canada, where consumers have a strong financial infrastructure and strong credit card options.

Despite their growing global popularity, it may be that using mobile payments systems is perceived as one of the riskier actions consumers can take with their mobile devices. Users are relying on third-party companies to mediate between retailers and service providers on the one hand and their banks or credit card companies on the

other. Thus, perceptions of the risk, trust, and benefit associated with these systems could play a major role in their adoption.

The purpose of our study was to assess the impact of perceived trust on consumer intent to adopt mobile payment systems. The extended valence framework from Kim et al. (2009) that incorporates net utility from perceived risk and perceived benefit was included in the new research model, along with three antecedents to trust, namely, privacy, security, and familiarity. Within the extended valence framework, we found positive significant relationships from trust to perceived benefit and from perceived benefit to intention to use. As consumer’s perceived trust increased, so did the perceived benefit they

Table 5 PLS-SEM construct measures

Construct	R <sup>2</sup>	Adjusted R <sup>2</sup>	Q <sup>2</sup>
Benefit	0.256	0.253	0.169
Intention	0.524	0.517	0.402
Risk	0.233	0.220	0.144
Trust	0.536	0.530	0.287

Table 6 PLS-SEM structural model results

Path	$\beta$	t value	p value	f <sup>2</sup>	VIF
Risk to intention	-0.082	1.516	0.130	0.014	1.037
Trust to intention	0.370	4.801	0.000	0.207	1.392
Trust to benefit	0.506	9.164	0.000	0.344	1.000
Trust to risk	0.153	1.110	0.268	0.014	2.153
Benefit to intention	0.446	6.645	0.000	0.310	1.349
Privacy to trust	-0.218	3.015	0.003	0.100	1.025
Privacy to risk	0.431	5.903	0.000	0.215	1.127
Security to trust	0.577	9.651	0.000	0.656	1.092
Security to risk	-0.310	2.747	0.006	0.069	1.807
Familiarity to trust	0.213	3.218	0.001	0.090	1.085
Familiarity to risk	0.025	0.306	0.760	0.001	1.183

**Table 7** Summary of hypothesis tests

Hypothesis	Supported
H1. A consumer's perceived risk negatively affects a consumer's intention to use Mobile Payment Systems.	No
H2. A consumer's perceived trust positively affects the consumer's intention to use Mobile Payment Systems.	Yes**
H3. A consumer's perceived trust positively affects the consumer's perceived benefit of Mobile Payment Systems.	Yes**
H4. A consumer's perceived trust negatively affects the consumer's perceived risk of Mobile Payment Systems.	No
H5. A consumer's perceived benefit positively affects a consumer's intention to use Mobile Payment Systems.	Yes**
H6. A consumer's perceived privacy concern negatively affects the consumer's perceived trust of Mobile Payment Systems.	Yes*
H7. A consumer's perceived privacy concern positively affects the consumer's perceived risk of Mobile Payment Systems.	Yes**
H8. A consumer's perceived security positively affects the consumer's perceived trust of Mobile Payment Systems	Yes**
H9. A consumer's perceived security negatively affects the consumer's perceived risk of Mobile Payment Systems.	Yes*
H10. A consumer's perceived familiarity positively affects the consumer's perceived trust of Mobile Payment Systems.	Yes*
H11. A consumer's perceived familiarity negatively affects the consumer's perceived risk of Mobile Payment Systems.	No

Note: significance levels: \* $p < .01$ , \*\* $p < .001$ ; two-tailed probabilities

saw in using mobile payment systems. As consumer's perceived benefit increased, so did their intention to use mobile payment systems. These relationships were hypothesized and supported. Another supported hypothesis we found was a significant positive relationship between perceived trust and intention to use. As consumer's perceived trust increased, so did their intention to use mobile payment systems. Overall, there is a very significant influence ( $p < .001$ ) between perceived trust and perceived benefit and between perceived trust and intention to use. However, our hypotheses were not supported when we evaluate perceived risk within the extended valence framework.

The relationship between perceived trust and perceived risk is not significant and the hypothesis was not supported. The relationship between perceived risk and intention to use was also not significant and the hypothesis was not supported. We turn to motivational avoidance theory to better explain these results. These systems and technologies are so complex, and users depend on them so much, that they have essentially given up worrying about potential risks involved in their use. As stated by Shepherd and Kay (2012), they "simply outsource personal responsibility to supposed qualified others." Chin et al. (2018) originally demonstrated the impact of motivational avoidance on risk in a valence framework. In their work, the relationships between trust and risk in a bi-directional model were insignificant both ways. In addition, the relationship between perceived risk and intention was also insignificant. The authors concluded motivational avoidance was

the contributing component and consumers simply relied on institutional dependence.

The three antecedents tested in this model were privacy concerns, security, and familiarity. All three had significant relationships with perceived trust, as hypothesized. In a negative relationship, as privacy concerns increased, perceived trust decreased. If a consumer has increased concerns about their privacy while using a mobile payment system, it makes sense their trust in the mobile payment system would decrease. Security had a significant positive relationship with trust. As a consumer perceives more security in their mobile payment system, the more they will trust the mobile payment system. Likewise, familiarity also had a positive significant relationship with trust. The more familiar a consumer is with the mobile payment system, the more they trust the mobile payment system.

For risk, privacy concerns and perceived security had significant relationships, as hypothesized. As privacy concerns increased, perceived risk increased. In a negative relationship, as perceived security increased, perceived risk decreased. Consumers feel mobile payments systems are riskier when they have more concerns with privacy, and they feel mobile payment systems are less risky when they believe security is enhanced. However, familiarity did not have a significant relationship with perceived risk, as it did with perceived trust. With trust, consumers were less trusting if they were less familiar. Contrarily, with risk, they did not perceive more risk if they were less familiar with the mobile payment system.

One potential explanation for this is that consumers are not as familiar with a mobile payment system when they first start using it as they are after using it a few times. As with most apps and new devices, there is a learning curve. Because consumers go through this often and frequently end up trusting the app or device, it may be that they do not inherently see increased risk at the beginning, knowing that they will likely become more familiar over time and will eventually trust the system. According to our results, consumers will not perceive increased risk at the beginning when they are less familiar with the mobile payment system, but they will perceive increased risk if they perceive privacy concerns or security threats.

To summarize, the purpose of this research was to assess the impact of trust, when balanced with risk and benefit, on consumer intention to adopt mobile payment systems. We used an extended valence framework and concluded that trust and benefit were the dominant constructs in determining the factors that influence consumer's adoption of mobile payment systems. We found that motivational avoidance theory played an important role in suppressing the risk construct, thus revealing consumer reliance on institutional dependence. Our antecedents of privacy, security, and familiarity all had significant relationships with trust, while security and privacy also had significant relationships with risk.

## 7.1 Research Implications

### 7.1.1 Practical and Managerial

The implications of this research affect all of the parties that engage in mobile payment systems. With the popularity of mobile devices and the expanding options for using mobile payment systems, there are positive benefits for consumers and vendors. From the consumer's perspective, they can make purchases or transfer money without needing cash, physically possessing a credit card, or going to the bank. They do not even need to carry a smartphone, as mobile payment services are now available on smart watches, smart rings, and bracelets. From the vendor perspective, they may be able to increase sales by catering to the convenience consumers seek. Providing mobile payment service options may help them capture consumers that might otherwise not make a purchase due to lack of cash. Impulse purchases by consumers may increase vendor revenue.

Mobile payment system vendors can also be encouraged that customers trust these systems and do not perceive that using them is overly risky. At the same time, this trust may be quite fragile, and any breach of security or privacy in a mobile payment system could dramatically

reduce this trust, sending users to other mobile payment platforms or to other payment technologies. A significant breach affecting one mobile payment system could jeopardize all other mobile payment systems by diminishing the trust consumers have in all such systems, not just the one suffering the breach. As other research has shown (Chin et al. 2018), users of mobile devices tend to trust the platforms that provide them goods and services, but if this trust is weakened, it could threaten the relationship consumers have with their vendors.

### 7.1.2 Theoretical

A primary contribution of this research is the use of the extended valence framework to investigate factors that influence the adoption of mobile payment systems. This is a new theoretical approach in mobile payment research, as much of the previous research has focused on TAM, UTAUT, and UTAUT2 (Harris et al. 2019). Another theoretical contribution is the introduction of motivational avoidance theory to mobile payment research. This is an important contribution with significant implications. Because consumers have institutional dependence, the risk construct has no significance with trust or intention to use mobile payment systems. Trust and benefit are the primary predictors.

## 7.2 Research Limitations and Future Research Directions

As with all research, our research has several limitations. First, all of the survey respondents in this study were college students, by definition having higher educational attainment than the general population. Second, the participants were young, with an average age of a little more than 22 years. Most of them are “digital natives” who are comfortable using technology to enhance many of their activities. Younger respondents may have different attitudes toward financial transactions than older people. It is important that similar studies be carried out with respondents from other age groups to determine if different outcomes prevail. Likewise, the respondents in this study were all from the United States, where consumers have more options when it comes to payment methods. Mobile payment systems are used more ubiquitously in many other countries, so the relationships revealed in the current study may be substantially different than in other countries where the financial system is configured differently. Future research directions include conducting studies that alleviate the limitations of a homogeneous population and of geography.

## Appendix

Construct	Survey question	Mean	Std Dev.
1. Perceived Security	1.1 Mobile payment systems will implement security measures to protect me.	4.98	1.250
	1.2 Mobile payment systems will protect my personal transaction information (e.g., credit card and/or bank account data).	4.89	1.315
	1.3 I will feel safe making transactions with mobile payment systems.	4.61	1.545
2. Perceived Privacy	2.1 I am concerned that the systems will collect too much personal information from me.	4.98	1.478
	2.2 I am concerned that the systems will use my personal information for other purposes without my approval.	4.60	1.613
	2.3 I am concerned that the systems will share my personal information with other entities without my authorization.	4.64	1.657
3. Familiarity	3.1 I am familiar with using a mobile payment system.	5.16	1.697
	3.2 I am familiar with the process of using a mobile payment system to send money.	4.99	1.758
	3.3 I am familiar with the process of using a mobile payment system to make purchases.	5.09	1.598
4. Perception of Risk	4.1 There is considerable risk involved in using mobile payment systems.	5.01	1.297
	4.2 There is a high potential for loss in using mobile payment systems.	4.60	1.380
	4.3 A decision to use mobile payment systems is risky.	4.65	1.341
5. Perception of Trust	5.1 Mobile payment systems are trustworthy.	4.47	1.135
	5.2 Mobile payment systems have my best interest in mind.	4.18	1.235
	5.3 Mobile payment systems have high integrity.	4.28	1.034
6. Perception of Benefit	6.1 Mobile payment systems can make my life easier.	5.73	1.146
	6.3 Mobile payment systems are useful.	5.80	1.082
	6.4 I can benefit from using mobile payment systems.	5.57	1.289
7. Intention to Use	7.1 I am likely to make a retail purchase or send money to others with a mobile payment system.	4.69	1.738
	7.2 I am likely to recommend using a mobile payment system to my friends.	4.82	1.719

## References

- Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Englewood Cliffs: Prentice Hall (Vol. 278).
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T).
- Alba, J. W., & Hutchinson, J. W. (1987). Dimensions of consumer expertise. *Journal of Consumer Research*, 13(4), 411. <https://doi.org/10.1086/209080>.
- Albashrawi, M., & Motiwalla, L. (2019). Privacy and personalization in continued usage intention of mobile banking: An integrative perspective. *Information Systems Frontiers*, 21(5), 1031–1043. <https://doi.org/10.1007/s10796-017-9814-7>.
- Aldás-Manzano, J., Ruiz-Mafé, C., & Sanz-Blas, S. (2009). Exploring individual personality factors as drivers of M-shopping acceptance. *Industrial Management & Data Systems*, 109(6), 739–757. <https://doi.org/10.1108/02635570910968018>.
- Aloudat, A., Michael, K., Chen, X., & Al-Debei, M. M. (2014). Social acceptance of location-based mobile government services for emergency management. *Telematics and Informatics*, 31(1), 153–171. <https://doi.org/10.1016/j.tele.2013.02.002>.
- Amoroso, D. L., & Magnier-Watanabe, R. (2012). Building a research model for mobile wallet consumer adoption: The case of mobile Suica in Japan. *Journal of Theoretical and Applied Electronic Commerce Research*, 7(1), 94–110. <https://doi.org/10.4067/S0718-18762012000100008>.
- Arora, R., & Stoner, C. (1996). The effect of perceived service quality and name familiarity on the service selection decision. *Journal of Services Marketing*, 10(1), 22–34. <https://doi.org/10.1108/08876049610106699>.
- Aydin, G. (2016). Adoption of mobile payment systems: a study on mobile wallets. *Pressacademia*, 5(1), 73–73. <https://doi.org/10.17261/pressacademia.2016116555>.
- Bélanger, F., & Carter, L. (2005). Trust and risk in e-government adoption. *Association for Information Systems – 11th Americas Conference on Information Systems, AMCIS 2005: A Conference on a Human Scale*, 2, 735–744. <https://doi.org/10.1016/j.jsis.2007.12.002>.
- Bélanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes Trustworthiness in electronic commerce: the role of privacy, security, and site attributes, 11(July 2016), 245–270. [https://doi.org/10.1016/S0963-8687\(02\)00018-5](https://doi.org/10.1016/S0963-8687(02)00018-5).



- Bisdikian, C., Gibson, C., Chakraborty, S., Srivastava, M. B., Sensoy, M., & Norman, T. J. (2014). Inference management, trust and obfuscation principles for quality of information in emerging pervasive environments. *Pervasive and Mobile Computing*, *11*, 168–187. <https://doi.org/10.1016/j.pmcj.2013.08.003>.
- Cao, X. (2017). Understanding mobile payment users' continuance intention: a trust transfer perspective, (71502168). <https://doi.org/10.1108/IntR-11-2016-0359>.
- Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management*, *15*, 358–368.
- Chin, A. G., Harris, M. A., & Brookshire, R. (2018). A bidirectional perspective of trust and risk in determining factors that influence mobile app installation. *International Journal of Information Management*, *39*. <https://doi.org/10.1016/j.ijinfomgt.2017.11.010>.
- Chin, A. G., Etudo, U., & Harris, M. A. (2016). On mobile device security practices and training efficacy: an empirical study. *Informatics in Education*, *15*(2), 235–252. <https://doi.org/10.15388/infedu.2016.12>.
- Chin, A. G., Little, P., & Jones, B. (2020). An analysis of smartphone security practices among undergraduate business students at a Regional Public University Amita G Chin Philip Little. *International Journal of Education and Development Using Information and Communication Technology*, *16*(1), 44–61.
- Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012). Measuring user confidence in smartphone security and privacy. *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12*, (1), 1. <https://doi.org/10.1145/2335356.2335358>.
- Cipriani, J. (2015). Here's why Samsung Pay is way better than Apple Pay and Android Pay. Retrieved October 14, 2019, from <https://fortune.com/2015/09/30/samsung-pay-review/>.
- Cocosila, M., & Trabelsi, H. (2016). Electronic commerce research and applications an integrated value-risk investigation of contactless mobile payments adoption. *Electronic Commerce Research and Applications*, *20*, 159–170. <https://doi.org/10.1016/j.elerap.2016.10.006>.
- Coupey, E., Irwin, J. R., & Payne, J. W. (1998). Product category familiarity and preference construction. *Journal of Consumer Research*, *24*(4), 459–468.
- Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. *Organization Science*, *10*(1), 104–115. <https://doi.org/10.1287/orsc.10.1.104>.
- Currás-Pérez, R., Ruiz-Mafé, C., & Sanz-Blas, S. (2013). Social network loyalty: Evaluating the role of attitude, perceived risk and satisfaction. *Online Information Review*, *37*(1), 61–82. <https://doi.org/10.1108/14684521311311630>.
- de Kerviler, G., Demoulin, N. T. M., & Zidda, P. (2016). Adoption of in-store mobile payment: Are perceived risk and convenience the only drivers? *Journal of Retailing and Consumer Services*, *31*, 334–344. <https://doi.org/10.1016/j.jretconser.2016.04.011>.
- Dahlberg, T., Guo, J., & Ondrus, J. (2015). A critical review of mobile payment research. *Electronic Commerce Research and Applications*, *14*(5), 265–284. <https://doi.org/10.1016/j.elerap.2015.07.006>.
- Dahlberg, T., Mallat, N., Ondrus, J., & Zmijewska, A. (2008). Past, present and future of mobile payments research: A literature review. *Electronic Commerce Research and Applications*, *7*(2), 165–181. <https://doi.org/10.1016/j.elerap.2007.02.001>.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340. <https://doi.org/10.2307/249008>.
- Dijkstra, T. K., & Henseler, J. (2015). Research essay consistent partial least squares path modeling. *MIS Quarterly*, *39*(2), 297–316.
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. <https://doi.org/10.1287/isre.1060.0080>.
- Ericsson. (2017). Mobility report. Accessed 24 Sept 2020. [Online]. Available: <https://www.Ericsson.Com/Res/Docs/2016/Ericsson-Mobility-Report-2016.Pdf>, (November), 7–8. <https://doi.org/10.3103/S0005105510050031>.
- Faden, M. (2020). QR Codes used in payment services. Retrieved May 22, 2020, from <https://www.americanexpress.com/us/foreign-exchange/articles/use-of-qr-codes-in-payment-services/>.
- Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Reading: Addison Wesley.
- Flavián, C., Guinalíu, M., & Gurrea, R. (2006). The role played by perceived usability, satisfaction and consumer trust on website loyalty. *Information and Management*, *43*(1), 1–14. <https://doi.org/10.1016/j.im.2005.01.002>.
- Gao, L., & Waechter, K. A. (2017). Examining the role of initial trust in user adoption of mobile payment services: an empirical investigation. *Information Systems Frontiers*, *19*(3), 525–548. <https://doi.org/10.1007/s10796-015-9611-0>.
- Gao, L., Waechter, K. A., & Bai, X. (2015). Understanding consumers' continuance intention towards mobile purchase: A theoretical framework and empirical study - A case of China. *Computers in Human Behavior*, *53*, 249–262. <https://doi.org/10.1016/j.chb.2015.07.014>.
- Gefen, D. (2000). E-commerce: the role of familiarity and trust. *Omega*, *28*(6), 725–737. [https://doi.org/10.1016/S0305-0483\(00\)00021-9](https://doi.org/10.1016/S0305-0483(00)00021-9).
- Goodwin, N. R. (1996). *Economic Meanings of Trust and Responsibility*. Ann Arbor: The University of Michigan Press.
- Grob, M. (2016). Impediments to mobile shopping continued usage intention: A trust-risk-relationship. *Journal of Retailing and Consumer Services*, *33*, 109–119. <https://doi.org/10.1016/j.jretconser.2016.08.013>.
- Gu, J., & Xu, Y. (Calvin), Xu, H., Zhang, C., & Ling, H. (2016). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems*. <https://doi.org/10.1016/j.dss.2016.10.002>.
- Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24. <https://doi.org/10.1108/EBR-11-2018-0203>.
- Harman, H. H. (1976). *Modern Factor Analysis* (3rd ed.). Chicago: University of Chicago Press.
- Harris, M. A., & Chin, A. G. (2016). Consumer trust in Google's top developers' apps: An exploratory study. *Information and Computer Security*, *24*(5). <https://doi.org/10.1108/ICS-11-2015-0044>.
- Harris, M. A., Chin, A. G., & Beasley, J. (2019). Mobile payment adoption: An empirical review and opportunities for future research. In *Southern Association of Information Systems 2019 Proceedings* (pp. 1–6). Retrieved from <https://aisel.aisnet.org/sais2019/8>.
- Harris, M. A., Chin, A. G., & Brookshire, R. (2015). Mobile app installation: The role of precautions and desensitization. *Journal of International Technology and Information Management*, *24*(4).
- Harris, M. A., Brookshire, R., & Chin, A. G. (2016). Identifying factors influencing consumers' intent to install mobile applications. *International Journal of Information Management*, *36*(3), 441–450. <https://doi.org/10.1016/j.ijinfomgt.2016.02.004>.
- Harris, M. A., & Patten, K. P. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security*, *22*(1), 97–114. <https://doi.org/10.1108/IMCS-03-2013-0019>.
- Hassoy, H., Durusoy, R., & Karababa, A. O. (2013). Adolescents' risk perceptions on mobile phones and their base stations, their trust to authorities and incivility in using mobile phones: a cross-sectional survey on 2240 high school students in Izmir, Turkey. *Environmental Health: A Global Access Science Source*, *12*(1), 10. <https://doi.org/10.1186/1476-069X-12-10>.

- Henseler, J., Ringle, C. M., & Sarstedt, M. (2014). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1), 115–135. <https://doi.org/10.1007/s11747-014-0403-8>.
- Hillman, S., & Neustaedter, C. (2016). Trust and mobile commerce in North America. *Computers in Human Behavior*, 70, 10–21. <https://doi.org/10.1016/j.chb.2016.12.061>.
- Infineon. (2017). Mobile payment, everything you need to know. Retrieved May 22, 2020, from <https://www.infineon.com/cms/en/discoveries/mobile-payment/>.
- Inscoc, S. (2017). Global consumer survey: consumer trust and security perceptions. Retrieved May 22, 2020, from <https://aitegroup.com/report/global-consumer-survey-consumer-trust-and-security-perceptions>.
- Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2020). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Information Systems Frontiers*. <https://doi.org/10.1007/s10796-020-10044-1>.
- Jacob, J., & Kaplan, L. B. (1972). The components of perceived risk. In M. Venkatesan (Ed.), *Proceedings of the Third Annual Conference of the Association for Consumer Research* (pp. 382–393). Chicago.
- Jing, Y., Ahn, G.-J., Zhao, Z., & Hu, H. (2014). Towards automated risk assessment and mitigation of mobile application. *IEEE Transactions on Dependable and Secure Computing*, 5971(c), 1–1. <https://doi.org/10.1109/TDSC.2014.2366457>.
- Johnson, E. J., & Russo, J. E. (1984). Product familiarity and learning new information. *Journal of Consumer Research*, 11(1), 542. <https://doi.org/10.1086/208990>.
- Jones, B. H., & Chin, A. G. (2015). On the efficacy of smartphone security: A critical analysis of modifications in business students' practices over time. *International Journal of Information Management*, 35(5), 561–571. <https://doi.org/10.1016/j.ijinfomgt.2015.06.003>.
- Jones, B. H., Chin, A. G., & Aiken, P. (2014). Risky business: Students and smartphones. *TechTrends*, 58(6), 73–83. <https://doi.org/10.1007/s11528-014-0806-x>.
- Jones, D. (2018). Smartwatch, bracelets help broaden mobile payment options amid competition. Retrieved October 1, 2020, from <https://www.mobilepaymentstoday.com/articles/smartwatch-bracelets-help-broaden-mobile-payment-options-amid-competition/>.
- Jonsson, P., Carson, S., Torres, A., Per Lindberg, K., & Karapantelakis, A. (2019). Ericsson mobility report. Retrieved May 22, 2020, from <https://www.ericsson.com/en/press-releases/2019/6/ericsson-mobility-report-5g-uptake-even-faster-than-expected>.
- Jorgensen, Z., Chen, J., Lafayette, W., Gates, C. S., Lafayette, W., & Proctor, R. W. (2015). Dimensions of risk in mobile applications: A user study. *Codaspy 2015*, 49–60. <https://doi.org/10.1145/2699026.2699108>.
- Jost, J. T., & Banaji, M. R. (1994). The role of stereotyping in system-justification and the production of false consciousness. *British Journal of Social Psychology*, 33(1), 1–27. <https://doi.org/10.1111/j.2044-8309.1994.tb01008.x>.
- Kapoor, K. K., Dwivedi, Y. K., & Williams, M. D. (2015). Examining the role of three sets of innovation attributes for determining adoption of the interbank mobile payment service. *Information Systems Frontiers*, 17(5), 1039–1056. <https://doi.org/10.1007/s10796-014-9484-7>.
- Kay, A. C., Gaucher, D., Napier, J. L., Callan, M. J., & Laurin, K. (2008). God and the government: testing a compensatory control mechanism for the support of external systems. *Journal of Personality and Social Psychology*, 95(1), 18–35. <https://doi.org/10.1037/0022-3514.95.1.18>.
- Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., & Abdullat, A. (2015). The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal*, 25(6), 637–667. <https://doi.org/10.1111/isj.12082>.
- Khalilzadeh, J., Ozturk, A. B., & Bilgihan, A. (2017). Security-related factors in extended UTAUT model for NFC based mobile payment in the restaurant industry. *Computers in Human Behavior*, 70(2017), 460–474. <https://doi.org/10.1016/j.chb.2017.01.001>.
- Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, 44(2), 544–564. <https://doi.org/10.1016/j.dss.2007.07.001>.
- Kim, D., Ferrin, D., & Rao, H. (2009). Trust and satisfaction, two stepping stones for successful e-commerce relationships: A longitudinal exploration. *Information Systems Research*, 20(2), 237–257. <https://doi.org/10.1287/isre.1080.0188>.
- Kim, G., & Koo, H. (2016). The causal relationship between risk and trust in the online marketplace: A bidirectional perspective. *Computers in Human Behavior*, 55, 1020–1029. <https://doi.org/10.1016/j.chb.2015.11.005>.
- Kim, K. K., & Prabhakar, B. (2004). Initial trust and the adoption of B2C e-commerce: The case of internet banking. *Data Base for Advances in Information Systems*, 35(2), 50–64. <https://doi.org/10.1145/1007965.1007970>.
- Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, 33(3), 22–42. <https://doi.org/10.1111/j.1540-4560.1977.tb01880.x>.
- 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. *Computers in Human Behavior*, 35, 464–478. <https://doi.org/10.1016/j.chb.2014.03.022>.
- 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. *Information and Management*, 48(8), 393–403. <https://doi.org/10.1016/j.im.2011.09.006>.
- Madden, T. J., Ellen, P. S., & Ajzen, I. (1992). A comparison of the theory of planned behavior and the theory of reasoned action. *Personality and Social Psychology Bulletin*, 18(1), 3–9. <https://doi.org/10.1177/0146167292181001>.
- Mallat, N. (2007). Exploring consumer adoption of mobile payments - A qualitative study. *Journal of Strategic Information Systems*, 16(4), 413–432. <https://doi.org/10.1016/j.jsis.2007.08.001>.
- Masclat, D., & Pénard, T. (2012). Do reputation feedback systems really improve trust among anonymous traders? An experimental study. *Applied Economics*, 44(35), 4553–4573. <https://doi.org/10.1080/00036846.2011.591740>.
- Matemba, E. D., Li, G., & Maiseli, B. J. (2018). Consumers' stickiness to mobile payment applications: An empirical study of wechat wallet. *Journal of Database Management*, 29(3). <https://doi.org/10.4018/JDM.2018070103>.
- McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: A trust building model. *Journal of Strategic Information Systems*, 11(3–4), 297–323. [https://doi.org/10.1016/S0963-8687\(02\)00020-3](https://doi.org/10.1016/S0963-8687(02)00020-3).
- Menke, L., & de Lussanet, M. (2006). SMS Based mobile payment: popular with the young. Retrieved October 14, 2019, from <http://www.forrester.com/Research/Document/Excerpt/0,7211,40678,00.html>.
- Meola, A. (2019). *Rise of M-Commerce: mobile ecommerce shopping stats & trends in 2020 business insider*. Retrieved May 22, 2020, from <https://www.businessinsider.com/mobile-commerce-shopping-trends-stats?op=1>.
- Miyazaki, A. D., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer Affairs*, 35(1), 27–44. <https://doi.org/10.1111/j.1745-6606.2001.tb00101.x>.
- Morosan, C., & DeFranco, A. (2016). It's about time: Revisiting UTAUT2 to examine consumers' intentions to use NFC mobile

- payments in hotels. *International Journal of Hospitality Management*, 53, 17–29. <https://doi.org/10.1016/j.ijhm.2015.11.003>.
- Nicolaou, A. I., & McKnight, D. H. (2006). Perceived information quality in data exchanges: Effects on risk, trust, and intention to use. *Information Systems Research*, 17(4), 332–351. <https://doi.org/10.1287/isre.1060.0103>.
- Oliveira, T., Thomas, M., Baptista, G., & Campos, F. (2016). Computers in human behavior mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology. *Computers in Human Behavior*, 61(2016), 404–414. <https://doi.org/10.1016/j.chb.2016.03.030>.
- Ozturk, A. B., Bilgihan, A., Salehi-Esfahani, S., & Hua, N. (2017). Understanding the mobile payment technology acceptance based on valence theory: A case of restaurant transactions. *International Journal of Contemporary Hospitality Management*, 29(8), 2027–2049. <https://doi.org/10.1108/IJCHM-04-2016-0192>.
- Park, C. W., & Lessig, V. P. (1981). Familiarity and Its impact on consumer decision biases and heuristics. *Journal of Consumer Research*, 8(2), 223. <https://doi.org/10.1086/208859>.
- Park, C. W., Kim, D., Gook, Cho, S., & Han, H. J. (2019). Adoption of multimedia technology for learning and gender difference. *Computers in Human Behavior*, 92(August 2018), 288–296. <https://doi.org/10.1016/j.chb.2018.11.029>.
- Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, 7(3), 69–103.
- Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research*, 15(1). <https://doi.org/10.1287/isre.1040.0015>.
- Pearson, S. (2013). *Privacy, security and trust in cloud computing, privacy and security for cloud computing*. London: Springer.
- Peter, J. P., & Tarpey, L. X. (1975). A comparative analysis of three consumer decision strategies. *Journal of Consumer Research*, 2(1), 29–37.
- Pietro, L., Di, Mugion, R., Mattia, G., Renzi, M. F., & Toni, M. (2015). The integrated model on mobile payment acceptance (IMMPA): an empirical application to public transport. *Transportation Research Part C: Emerging Technologies*, 56, 463–479. <https://doi.org/10.1016/j.trc.2015.05.001>.
- Pinola, M. (2018). Lifewire: How to pay with your phone or tablet. Retrieved October 14, 2019, from <https://www.lifewire.com/mobile-payments-4103869>.
- Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & 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), 879–903. <https://doi.org/10.1037/0021-9010.88.5.879>.
- Qasim, H., & Abu-Shanab, E. (2016). Drivers of mobile payment acceptance: The impact of network externalities. *Information Systems Frontiers*, 18(5), 1021–1034. <https://doi.org/10.1007/s10796-015-9598-6>.
- Qiu, M., Li, R., & Chen, M. (2013). An influence study on adopting will of tourism mobile e-commerce by the perceived risk and trust. *IBusiness*, 05(01), 39–42. <https://doi.org/10.4236/ib.2013.51B009>.
- Quelch, J. A., & Klein, L. R. (1996). The internet and international marketing. *Sloan Management Review*, 37(3).
- Rao, A. R., & Monroe, K. B. (1988). The moderating effect of prior knowledge on cue utilization in product evaluations. *Journal of Consumer Research*, 15(2), 253. <https://doi.org/10.1086/209162>.
- Ringle, C. M., Wende, S., & Becker, J.-M. (2015). *SmartPLS 3*. Boenningstedt: SmartPLS GmbH.
- Schierz, P. G., Schilke, O., & Wirtz, B. W. (2010). Understanding consumer acceptance of mobile payment services: An empirical analysis. *Electronic Commerce Research and Applications*, 9(3), 209–216. <https://doi.org/10.1016/j.elerap.2009.07.005>.
- Shepherd, S., & Kay, A. C. (2012). On the perpetuation of ignorance: system dependence, system justification, and the motivated avoidance of sociopolitical information. *Journal of Personality and Social Psychology*, 102(2), 264–280. <https://doi.org/10.1037/a0026272>.
- Shin, D. H. (2009). Towards an understanding of the consumer acceptance of mobile wallet. *Computers in Human Behavior*, 25(6), 1343–1354. <https://doi.org/10.1016/j.chb.2009.06.001>.
- Shin, D. H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with Computers*, 22(5), 428–438. <https://doi.org/10.1016/j.intcom.2010.05.001>.
- Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146–164. <https://doi.org/10.1016/j.comnet.2014.11.008>.
- Slade, E. L., Dwivedi, Y. K., Piercy, N. C., & Williams, M. D. (2015). Modeling consumers' adoption intentions of remote mobile payments in the United Kingdom: Extending UTAUT with innovativeness, risk, and trust. *Psychology & Marketing*, 32(8), 860–873. <https://doi.org/10.1002/mar>.
- Sorensen, E. (2018). Different types of mobile payment explained. Retrieved October 14, 2019, from <https://www.mobiletransaction.org/different-types-of-mobile-payments/>.
- Suh, B., & Han, I. (2003). The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of Electronic Commerce*, 7(3), 135–161. <https://doi.org/10.1080/10864415.2003.11044270>.
- Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research*, 6(2), 144–176. <https://doi.org/10.1287/isre.6.2.144>.
- Thakur, R., & Srivastava, M. (2014). Adoption readiness, personal innovativeness, perceived risk and usage intention across customer groups for mobile payment services in India. *Internet Research*, 24(3), 369–392. <https://doi.org/10.1108/IntR-12-2012-0244>.
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425–478.
- Viswanathan, P. (2018). Lifewire: 8 popular mobile payment apps. Retrieved October 14, 2019, from <https://www.lifewire.com/most-popular-mobile-payment-apps-2373179>.
- Warkentin, M., Gefen, D., Pavlou, P. A., & Rose, G. M. (2002). Encouraging citizen adoption of e-government by building trust. *Electronic Markets*, 12(3), 157–162.
- Wu, J. H., & Wang, S. C. (2005). What drives mobile commerce? An empirical evaluation of the revised technology acceptance model. *Information and Management*, 42(5), 719–729. <https://doi.org/10.1016/j.im.2004.07.001>.
- Yan, Z., Dong, Y., Niemi, V., & Yu, G. (2013). Exploring trust of mobile applications based on user behaviors: An empirical study. *Journal of Applied Social Psychology*, 43(3), 638–659. <https://doi.org/10.1111/j.1559-1816.2013.01044.x>.
- Yan, Z., Zhang, P., & Deng, R. H. (2012). TruBeRepec: A trust-behavior-based reputation and recommender system for mobile applications. *Personal and Ubiquitous Computing*, 16(5), 485–506. <https://doi.org/10.1007/s00779-011-0420-2>.
- Yang, C. G., & Lee, H. J. (2016). A study on the antecedents of healthcare information protection intention. *Information Systems Frontiers*, 18(2), 253–263. <https://doi.org/10.1007/s10796-015-9594-x>.
- Yang, H. (2013). Young American consumers' online privacy concerns, trust, risk, social media use, and regulatory support. *Journal of New Communications Research*, 5(1), 1–30.
- Yang, S., Cao, Y., Mao, W., Zhang, R., & Luo, L. (2011). Determinants of behavioral intention to mobile payment: Evidence from China. In *7th International Conference on Advanced Information Management and Service (ICIPM)* (pp. 151–154). IEEE.